TightGate®-Pro

Dediziertes Remote-Controlled Browser System
zum Schutz vor Gefahren aus dem Internet

Administrationshandbuch

m-privacy_AGD-OPE
Build 1.4-780

Herausgeber:
m-privacy GmbH
Technische Redaktion
Werner-Voß-Damm 62
12101 Berlin

Fon: +49 30 243423-34
Fax: +49 30 99296856

support@m-privacy.de
help.m-privacy.de/tightgate-pro

Inhaltsverzeichnis

Versionshistorie

Ver.	Datum	Änderung	Redakteur
1.00	21.09.2011	Dokument erstellt	ple
1.02	27.09.2011	Änderung: redaktionelle Änderungen	ple
1.03	30.09.2011	Änderung: config > Einstellungen > 3D-Hardware-X-Server* nicht mehr CC-relevant.	ple
1.10	02.03.2012	Änderung: Änderungen bis Build 1.4-353	ple
1.11	22.03.2012	Ergänzung: Viewer und Schleuse für Apple Macintosh / OS X	ple
1.12	23.03.2012	Ergänzung: Notwendigkeit zum Betrieb eines DNS-Servers	ple
1.13	19.04.2012	Ergänzung: Installation des Antivirusprogramms F-Prot	ple
1.14	20.04.2012	Ergänzung: weitere Profile für CSV-Import	ple
1.15	27.04.2012	Ergänzung: Statusseite	ple
1.16	03.05.2012	Änderung: Änderungen bis Build 1.4-379	ple
1.17	07.05.2012	Ergänzung: Anhang Nagios-Systemüberwachung	ple
1.18	06.06.2012	Änderung: Update-Verfahren HTTP-Proxy entfernt.	ple
1.19	14.06.2012	Änderung: Detailkorrekturen 10.2 / 10.3	ple
1.20	27.07.2012	Änderung: durchgängige Präzisierung der Bezeichnung TOE	ple
1.30	31.10.2012	Änderung: Änderungen bis Build 1.4-444	ple
1.31	14.11.2012	Änderung: Fehlerkorrektur SSH-Server	ple
1.40	25.01.2013	Änderungen / Ergänzungen	ple
1.45	14.02.2013	Redaktionelle Fehlerbereinigung	ple
1.50	18.02.2013	Änderungen / Ergänzungen	ple
1.51	19.02.2013	Rollenberechtigungen neu gefasst	ple
1.53	25.03.2013	Ergänzung: Vorbereitung von Festplatten zum Backup	ple
1.55	03.04.2013	Ergänzung: Hinweise zur Audioübertragung	ple
1.56	02.05.2013	Redaktionelle Fehlerbereinigung	ple
1.60	28.05.2013	Informationen zu Active Directory hinzugefügt.	ple
1.65	04.06.2013	Änderung: Änderungen bis Build 1.4-506b	ple
1.66	03.07.2013	Ergänzung: Nagios-Check	ple
1.70	16.07.2013	Ergänzung: AD-Einbindung, CSV-Import und zentraler GnuPG-Key. Änderungen Reihenfolge der MIME-Typen, kleinere Korrekturen.	HOM
1.75	26.07.2013	Konsolidierung von Änderungen / Fehlerkorrekturen	ple
1.80	27.08.2013	Ergänzung: AD-Einbindung / Fehlerkorrekturen	HOM
1.85	28.08.2013	Konsolidierung von Änderungen / Fehlerkorrekturen	ple
1.86	28.10.2013	Korrekturen: AD-Einbindung	HOM
1.87	04.12.2013	Korrektur: Tabelle in 5.5.1 ergänzt um letzte Spalte	ple
1.90	05.12.2013	Anhang ausgelagert, Titelei geändert	ple
1.91	20.01.2014	Unternehmensanschrift geändert	ple
1.92	19.02.2014	Änderung: Änderungen bis Build 1.4-607	ple

Ver.	Datum	Änderung	Redakteur
1.93	06.03.2014	Detailkorrekturen	ple
2.00	14.11.2014	Änderung: Änderungen bis Build 1.4-705	ple
2.10	21.01.2015	Änderung: Änderungen bis Build 1.4-737	ple
2.20	28.01.2015	Neufassung und Zusammenlegung der Kapitel 6 und 7	ple
2.21	30.01.2015	Reduktion Kap. 6 / Verschiebung nach Kap. 4	ple
2.30	30.03.2015	Ergänzung Viewer und Schleuse für Apple OS X	ple
2.31	13.05.2015	Änderung Passwort für Revision	hom
2.40	10.06.2015	Änderung: Änderungen bis Build 1.4-780	ple

Allgemeine Hinweise zu diesem Handbuch

Alle Materialien und Ausführungen wurden mit Sorgfalt erarbeitet und zusammengestellt. Dennoch sind Fehler nicht auszuschließen. Die m-privacy GmbH übernimmt keine Haftung für Schäden, die aus Unrichtigkeit einzelner Angaben entstehen.

Im Sinne einer raschen Orientierung und zur Vermeidung von Sicherheitsrisiken werden besonders wichtige Aspekte durch wiederkehrende Stichworte gekennzeichnet. Diese sind:

Hinweis
Unter diesem Stichwort werden nützliche Details zur rationellen Verwendung von TightGate®-Pro erläutert.

Achtung
Unter diesem Stichwort erfolgen Hinweise zur Problemvermeidung bzw. zur Vorbeugung von Betriebsstörungen bei TightGate®-Pro.

Warnung
Unter diesem Stichwort erfolgen Hinweise auf mögliche Fehler bei der Konfiguration und Verwendung von TightGate®-Pro, die weitreichende Sicherheitsrisiken bergen oder zu schwerwiegenden Betriebsstörungen führen können.

Hinweise zu den Ergänzungsspalten der tabellarischen Darstellungen

Die tabellarischen Darstellungen der Einstelloptionen tragen die Ergänzungsspalten C, E und F. Die Bedeutung der darin enthaltenen Codes ist dem Anhang 15.6 zu entnehmen.

Hinweis: Die mit einem Stern (*) gekennzeichneten Einstelloptionen betreffen in Verbundrechnersystemen (Clustersystemen) sämtliche Einzelrechner (Nodes) gleichermaßen.

1 Einführung

Das dedizierte Remote-Controlled Browser System (ReCoBS) TightGate®-Pro schützt präventiv vor Angriffen aus dem Internet und erweist sich damit regelmäßig als wirksamer als jedes filternde System wie Malware-Scanner, Firewalls oder Intrusion Detection Systems (IDS). Es handelt sich um ein dediziertes Schutzsystem, das als Appliance dem internen Unternehmens- oder Behördennetzwerk vorgeschaltet wird. Internetgebundene Applikationen wie beispielsweise der Internetbrowser werden nicht mehr auf dem Arbeitsplatzrechner, sondern auf TightGate®-Pro Server ausgeführt. Deren Zugriffe in das Internet erfolgen ausschließlich vom vorgeschalteten Schutzsystem aus. Lediglich die Bildschirmausgabe der betreffenden Programme wird in das interne Netzwerk übertragen und auf den Arbeitsplatzrechnern angezeigt. Zugleich werden Maus- und Tastaturinformationen von den Arbeitsplatzrechnern an TightGate®-Pro Server übermittelt und die dort ausgeführten Programme aus sicherer Distanz ferngesteuert. Zur Datenübertragung dient vorrangig ein funktionsspezifisches VNC-Protokoll mit dem Übertragungsstandard RFB (Remote Frame Buffer). Das entsprechende Viewer-Programm (VNC-Viewer) wird seitens der m-privacy GmbH in speziell angepassten und optimierten Versionen lizenzkostenfrei zur Verfügung gestellt.

TightGate®-Pro bietet volle Internetfunktionalität auch in kritischen Infrastrukturen und Betriebsumgebungen mit hohem Schutzbedarf. Das System unterbindet infolge der physikalischen Trennung von der „Gefahrenquelle Internet“ zuverlässig jede Form von Angriffen auf die Arbeitsstation und das interne Netzwerk, wie sie beispielsweise infolge von Sicherheitslücken in internetgebundenen Applikationen realisierbar sind. Die Nutzung aktiver Inhalte sowie die Wiedergabe von Multimediainhalten ist dennoch vollumfänglich und ohne Gefährdung interner Ressourcen möglich. TightGate®-Pro Server verfügt weiterhin über einen starken Eigenschutz durch das Konzept der „administrativen Gewaltenteilung“ (rollenbasierte Administration ohne Root- oder Superuser-Konto) in Verbindung mit feingranularer Zugriffsrechtekontrolle und starker Härtung des zugrunde liegenden Serverbetriebssystems nach dem aktuellen Stand der IT-Sicherheitstechnik.

Dieses Administrationshandbuch dient als Anleitungs- und Nachschlagewerk für alle, die sich mit der Konfiguration und Verwaltung von TightGate®-Pro befassen. Erläuterungen, Hinweise, Warnungen und Tabellen schildern die korrekte Verwendung des Schutzsystems und unterstützen den Administrator bei der Vermeidung von Sicherheitsrisiken infolge fehlerhafter Konfiguration oder Nutzung. Ergänzende Hintergrundinformationen ermöglichen es, die Leistungsfähigkeit von TightGate®-Pro voll auszuschöpfen und auch auf seltenere Spezialfälle im Produktivbetrieb angemessen zu reagieren.

Im Rahmen der folgenden Erläuterungen wird zwischen Benutzern und Administratoren unterschieden. Benutzer melden sich ausschließlich an der grafischen Benutzeroberfläche über die Viewer-Software an TightGate®-Pro Server an. Ein Benutzer des dedizierten ReCoB-Systems TightGate®-Pro ist in der Lage, mit dem Internetbrowser auf Webinhalte zuzugreifen, Textinhalte über die Zwischenablage zwischen TightGate®-Pro Server und dem eigenen Arbeitsplatzrechner auszutauschen sowie optional den Audiokanal zur Tonwiedergabe zu nutzen (z. B. zur Wiedergabe von Multimediainhalten). Weiterhin besteht für Benutzer die technische Möglichkeit zum Dateiaustausch zwischen TightGate®-Pro Server und dem eigenen Arbeitsplatzrechner über eine gesicherte Dateischleuse. Im Bedarfsfall kann der Benutzer in Eigenregie auf Sicherungskopien eigener Daten zugreifen und diese zurückspielen.

Administratoren arbeiten im Verwaltungsbereich von TightGate®-Pro Server und nutzen regelmäßig Konsolenzugänge über SSH. Für die speziellen Administratorenrollen ***root*** und ***security*** (bei TightGate®-Pro (CC) Version 1.4 Server nur im sogenannten Softmode verfügbar) muss der Administratorenzugang über SSH vor Benutzung explizit freigegeben werden. Administratorenzugänge direkt an der Konsole (am Gerät) sind in jedem Fall und zeitlich unbegrenzt möglich.

1.1 TightGate®-Pro und TightGate®-Pro (CC) Version 1.4

Das ReCoB-System TightGate®-Pro ist in zwei Varianten verfügbar. Diese sind TightGate®-Pro für Standardumgebungen (im Folgenden nur als „TightGate®-Pro“ bezeichnet) und TightGate®-Pro (CC) Version 1.4 für CC-konforme Umgebungen. TightGate®-Pro (CC) Version 1.4 unterscheidet sich von TightGate®-Pro für Standardumgebungen maßgeblich durch einige Voreinstellungen sowie die Handhabung des Dateiaustauschs zwischen Server und Klientenrechner:

- TightGate®-Pro (CC) Version 1.4 Server wird mit werkseitig deaktiviertem Textaustausch via Zwischenablage ausgeliefert. Diese Einstellung kann durch den Administrator config geändert werden. Das Viewer-Programm TightGate®-Pro (CC) Version 1.4 Client wird werkseitig mit der Voreinstellung zur Einzelbestätigung eines jeden Texttransfers ausgeliefert.
- Die Administrationsrollen ***root*** und ***security*** sind auch in TightGate®-Pro (CC) Version 1.4 Server vorhanden, können sich jedoch nur im sogenannten Softmode (bei deaktivierter RSBAC-Kontrolle) anmelden. Zugleich wird der VNC-Server aus Sicherheitsgründen deaktiviert, sodass eine Anmeldung von Klienten über den Viewer nicht möglich ist.

Hinweis: Weitere Detailunterschiede werden bei den jeweiligen Einstelloptionen erläutert.

Achtung: TightGate®-Pro Server und TightGate®-Pro (CC) Version 1.4 Server dürfen nur mit Viewer-Programmen (Klienten) der m-privacy GmbH verwendet werden. TightGate®-Pro Client beziehungsweise TightGate®-Pro (CC) Version 1.4 Client sind daher obligatorisch, alternative Viewer-Programme sind nicht nutzbar. Die Systemadministration muss sicherstellen, dass Installation und Betrieb alternativer Klientenprogramme (VNC-Viewer) auf den Arbeitsplatzrechnern (Klientenrechnern) nicht möglich sind. Ein CC-konformes Gesamtsystem ergibt sich nur in der Kombination TightGate®-Pro (CC) Version 1.4 Server und TightGate®-Pro (CC) Version 1.4 Client.

1.2 Netzwerkplanung

TightGate®-Pro Server wird regelmäßig in der so genannten Demilitarisierten Zone (DMZ) unmittelbar hinter der ersten Firewall in die Unternehmens- bzw. Behördeninfrastruktur integriert. Sollte dies aus technischen oder organisatorischen Gründen nicht möglich sein, steht unter sicherheitstechnischen Gesichtspunkten auch einer direkten Verbindung des Schutzsystems mit dem Internet nichts entgegen. Der starke Eigenschutz des ReCoBS-Servers verhindert negative Einflüsse auf das Schutzniveau weitestgehend.

Arbeitsplatzrechner aus dem internen Netz können die sicheren Dienste des ReCoBS-Servers nutzen. Zugleich ist durch Vorschaltung geeigneter Paketfilter sicherzustellen, dass sich die Arbeitsplatzrechner bzw. die darauf installierten internetgebundenen Applikationen (Internetbrowser, E-Mail-Programm und dergleichen) nicht mehr direkt mit dem Internet außerhalb des internen Netzwerks verbinden können. Der Übergang zum Internet erfolgt ausschließlich über TightGate®-Pro Server. Im Bedarfsfall können Direktverbindungen zu vertrauenswürdigen Gegenstellen (Online-Banking, VPN etc.) administrationsseitig zugelassen werden, sofern Angriffe auf das interne Netzwerk über diese Verbindungen mit genügender Sicherheit ausgeschlossen werden können.

1.3 Umfeldmaßnahmen

Der sichere Betrieb von TightGate®-Pro und die damit erzielbare Schutzwirkung auf Arbeitsplatzrechner und das sie umgebende Netzwerk können durch das IT-Umfeld von TightGate®-Pro Server sowie der Klientenrechner (Arbeitsplatzstationen) beeinflusst werden.

1.3.1 Absicherung der Arbeitsplatzrechner (Klientenrechner)

Arbeitsplatzrechner (Klientenrechner), von denen aus über TightGate®-Pro auf das Internet zugegriffen werden soll, dürfen keine anderweitige Verbindung zum Internet haben. Die Netzwerkverbindung der Klientenrechner ist über entsprechend konfigurierte Paketfilter bzw. Firewalls vom Internet abzuschotten. Erforderlichenfalls ist für adäquaten Malware-Schutz im internen Netzwerk sowie auf den Klientenrechnern zu sorgen, falls eine Gefährdungsanalyse einen entsprechenden Bedarf erkennen lässt.

Es ist darauf zu achten, dass Benutzer die Klientenrechner nur mit eingeschränkten Benutzerrechten verwenden. Seitens der Systemadministration muss sichergestellt sein, dass TightGate®-Pro Client durch den Benutzer nicht mit Administratorrechten gestartet wird, um eine dauerhafte Verankerung unbeabsichtigter oder unberechtigter Änderungen von Konfigurationseinstellungen an TightGate®-Pro Client (Viewer-Programm) zu unterbinden.

Die Nutzung von TightGate®-Pro Server ist nur mit TightGate®-Pro Client, dem dafür vorgesehenen Viewer-Programm, zu bewerkstelligen. Andere VNC-Viewer-Programme können sich entweder aufgrund fehlender Funktionalität (z. B. Verschlüsselungsverfahren) nicht mit TightGate®-Pro Server verbinden oder erfüllen nicht die Anforderungen im Hinblick auf bestimmte Sicherheitsvorkehrungen beziehungsweise Verfahrensvorgaben. Die Systemadministration muss sicherstellen, dass Installation und Betrieb alternativer Klientenprogramme (VNC-Viewer) auf den Arbeitsplatzrechnern (Klientenrechnern) nicht möglich sind.

Warnung: TightGate®-Pro bietet systembedingt keinen Schutz vor Angriffen, die über anderweitig freigegebene Netzwerkkanäle auf die Klientenrechner oder das diese umgebende interne Netzwerk einwirken. Grundlegende Maßnahmen zum Schutz der Betriebsumgebung von TightGate®-Pro Server vor Manipulationen sind seitens der Systemadministration des internen Netzwerks zu ergreifen.

1.4 Eigensicherheit von TightGate®-Pro Server

TightGate®-Pro Server verfügt über weitreichende Mechanismen zum Eigenschutz im Hinblick stabilen und sicheren Dauerbetrieb.

1.4.1 Serverbetriebssystem und Kommunikationsprotokoll

Das Serversystem verfügt ausschließlich über solche Programmkomponenten, die für dessen Betrieb unabdingbar sind. Eine umfassende Kapselung sämtlicher Programme und Prozesse beugt einer unkontrollierten Ausführung nicht autorisierter Software sowie eine Manipulation installierter Programmkomponenten auf dem Serverrechner wirksam vor. Ein funktionsspezifisches Kommunikationsprotokoll zwischen TightGate®-Pro Server und TightGate®-Pro Client verhindert zuverlässig den unkontrollierten Zugriff in das interne Netzwerk und aus diesem heraus.

1.4.2 Abschottung von Benutzerkonten

Sämtliche Benutzerkonten und die durch angemeldete Benutzer (VNC-Benutzer) initiierten Benutzersitzungen (Sessions) sind auf TightGate®-Pro Server vollständig voneinander abgeschottet. Es besteht keine Möglichkeit eines wechselseitigen Zugriffs oder einer Beeinflussung. Reguläre VNC-Benutzer können nicht mit Administratorberechtigungen ausgestattet werden, die über die Benutzerrolle hinausgehende Handlungsoptionen eröffnen.

1.4.3 Sichere Startbedingungen

TightGate®-Pro Client startet bei jedem Aufruf in einem sicheren Ausgangszustand. Wesentliche Sicherheitsoptionen sind serverseitig fixiert. Nachgeordnete Konfigurationsänderungen, beispielsweise durch Einstellungen im Programmmenü von TightGate®-Pro Client, werden im Benutzerkontext nicht dauerhaft gespeichert und nach Beendigung der Benutzersitzung (Session) auf die vorgegebenen Standardwerte zurückgesetzt. Weiterhin bleiben auf TightGate®-Pro Server keine aktiven Inhalte aus einer Internetsitzung nach deren Beendigung erhalten. Alle auf TightGate®-Pro Server im Benutzerkontext gestarteten Programme und Applikationen werden bei der Abmeldung von TightGate®-Pro Server automatisch beendet. Eine wechselseitige Beeinflussung von Applikationen auf TightGate®-Pro Server, insbesondere im Hinblick auf den verwendeten Internetbrowser, ist durch vollständige Kapselung aller Softwarekomponenten in separaten Berechtigungssphären ausgeschlossen.

1.4.4 Mehrdimensionale Systemhärtung und Fehlerresistenz

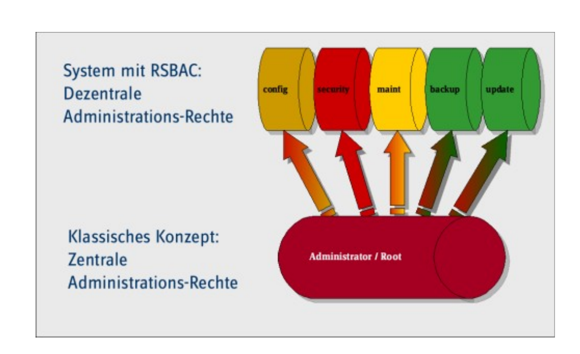
Die Kombination unterschiedlicher Härtungs- und Kapselungsmaßnahmen zum Eigenschutz von TightGate®-Pro Server nach dem Stand der Technik in Verbindung mit einem funktionsspezifischen Protokoll zur Kommunikation mit den Klientenrechnern bewirkt ein außerordentliches Maß an sicherheitstechnischer Robustheit. Dies gilt insbesondere auch unter der A-Priori-Annahme, dass einzelne Programmkomponenten von TightGate®-Pro Server oder TightGate®-Pro Client mit Unzulänglichkeiten hinsichtlich Programmlogik respektive Implementierung behaftet sein könnten.

Im Zuge der Installation von TightGate®-Pro Server oder TightGate®-Pro Client sind daher keine über die im Abschnitt 1.4 beschriebenen Maßnahmen erforderlich, um das vorgesehene Schutzniveau zu erzielen.

1.5 Das Administrationskonzept von TightGate®-Pro Server

TightGate®-Pro Server hat werkseitig fest vordefinierte Administratorenrollen, die den herkömmlichen Administrator (root) ersetzen. Keine dieser Administratorenrollen verfügt über umfassende Zugriffsrechte auf das Gesamtsystem (Superuser-Privilegien). Die Vorteile dieses dezentralen Administrationskonzepts ist einerseits der Schutz des Systems und der Benutzerdaten vor einer funktional unangemessen Allmacht[1]. Anderseits wird durch die Abbildung einzelner Administrationsvorgänge auf mehrere Rollen eine Delegation der Aufgaben möglich. Die konkreten Berechtigungen der jeweiligen Rollen sind im Anhang zu diesem Administrationshandbuch tabellarisch zusammengefasst.

Warnung:
Generell ist anzumerken, dass die Verwaltung TightGate®-Pro Server oder TightGate®-Pro (CC) Version 1.4 Server ausschließlich von vertrauenswürdigen und hinreichend ausgebildeten, sicherheitsbewussten Fachkräften vorzunehmen ist. TightGate®-Pro Server oder TightGate®-Pro (CC) Version 1.4 Server können einem durch Fehlbedienung oder Fehlkonfiguration bedingten Sicherheitsrisiko nicht oder nur sehr bedingt entgegentreten. Vor diesem Hintergrund sind auch die mit dem Schlüsselwort **Warnung** gekennzeichneten Passagen dieser Dokumentation besonders zu beachten.



Alle Viewer-Programme (VNC-Viewer) müssen gegen gängige Manipulationsversuche auf den Klientenrechnern (Arbeitsplatzrechnern) gesichert werden, beispielsweise durch eine restriktive Berechtigungsvergabe.

Auf die Benutzer ist einzuwirken, dass die Verwendung gleicher Zugangsdaten für TightGate®-Pro Server oder TightGate®-Pro (CC) Version 1.4 Server und weiteren Netzwerkdiensten vermieden wird. Darüber hinaus sind alle Maßnahmen zu ergreifen, die der guten Praxis und dem Stand der Technik in Fra-

1 Die herkömmliche Konzentration aller Administrationsaufgaben und Systemrechte in einem zentralen Account gefährdet diesen in besonderem Maße im Bezug auf Eindringversuche. Unbefugte, die Zugang zu einem solchen Benutzerkonto erlangen, erhalten Zugriff auf das gesamte System.

gen der IT-Sicherheit entsprechen, unabhängig vom Einsatz von TightGate®-Pro oder TightGate®-Pro (CC) Version 1.4.

Hinweis:
Im Folgenden wird für TightGate®-Pro Server oder TightGate®-Pro (CC) Version 1.4 Server einheitlich „TightGate®-Pro Server“ verwendet, sofern die jeweiligen Ausführungen für beide Varianten des ReCoBS-Servers bzw. des VNC-Viewers gelten. Unterschiede sind den Erläuterungen zu entnehmen.

1.5.1 Systembezogene Administration

Für die System- und Sicherheitsadministration von TightGate®-Pro Server wurde das Administratorkonto ***config*** geschaffen. Dieses ist zuständig für die Netzwerkeinstellungen und systemweite Vorgaben z. B. für Benutzerkonten. Keinen Zugriff hingegen hat diese Administrationsrolle auf Benutzerverzeichnisse und Benutzereinstellungen. Die meisten Wartungsaufgaben können damit datenschutzrechtlich bedenkenlos unterbeauftragt werden.

1.5.2 Personenbezogener Bereich

Dem Administrationsaccount ***maint*** obliegt die Benutzerverwaltung von TightGate®-Pro Server. Es können Benutzer angelegt, Zugangsberechtigungen und -einschränkungen vorgenommen und Passwörter geändert werden. Dieser Administrator hat ebenfalls die Möglichkeit, einzelne Dienste neu zu starten und ggf. einen Fernwartungszugang freizuschalten. Eine inhaltliche Kontrolle von Benutzerverzeichnissen und -daten durch ***maint*** ist ausgeschlossen.

1.5.3 Wartungsbereich

Für Wartungsaufgaben von TightGate®-Pro Server wurden die Administratorkonten ***backuser*** und ***update*** vorgesehen. Sie haben nur einen sehr begrenzten Funktionsumfang und speziell definierte Rechte. Dabei ist der ***backuser*** ausschließlich für das Erstellen und Verwalten von Backups und die dafür notwendigen Einstellungen verantwortlich. Gleiches gilt für die Rolle ***update*** bei der Pflege des Systems. Beide Rollen haben weder Zugriff auf die Netzwerkeinstellung noch dürfen sie Benutzerverzeichnisse einsehen.

1.5.4 Sicherheitsbereich

Die zentrale Sicherheit von TightGate®-Pro Server wird über den Zugriffsrechteschutz RSBAC gewährleistet. Die RSBAC-Konfiguration ist bei Auslieferung komplett konfiguriert und darf regelmäßig nicht von Administratoren verändert werden. Zur Bearbeitung der RSBAC-Sicherheitseinstellungen gibt es die Administratoren ***root*** und ***security***. Beide sind standardmäßig deaktiviert.

Hinweis: In TightGate®-Pro (CC) Version 1.4 Server für CC-konforme Umgebungen sind die Administrationsrollen ***root*** und ***security*** nur im verfügbar, wenn das System im Softmode gestartet wird.

1.5.5 Benutzerbereich

Anwender, die sich über ein Viewer-Programm (VNC-Viewer) an der grafischen Benutzeroberfläche von TightGate®-Pro Server oder TightGate®-Pro (CC) Version 1.4 Server anmelden, werden Benutzer genannt. Dies unterscheidet sie von den Administratoren, die sich über Konsolenzugänge mit TightGate®-Pro Server oder TightGate®-Pro (CC) Version 1.4 Server verbinden und administrative Aufgaben wahrnehmen. Benutzer benötigen ein Viewer-Programm (VNC-Viewer) auf ihrem Arbeitsplatzrechner, mit dem sie sich mit TightGate®-Pro Server verbinden. Dieses Viewer-Programm wird seitens der m-privacy GmbH bereitgestellt und kann lizenzkostenfrei bezogen werden. Es darf auf beliebig vielen Arbeitsplatzrechnern installiert werden. Alternative VNC-Viewer sind nicht verwendbar.

Hinweis: Ein Benutzer kann auf TightGate®-Pro Server generell keine Administratorrechte ausüben und darf die betreffenden Einstellmenüs von Administratorrollen nicht einsehen. Administratorrechte können nicht auf einen Benutzer übertragen werden, die Berechtigungen des Benutzers sind bei TightGate®-Pro Server auch nicht über Einstelloptionen erweiterbar. Administrative Eingriffe müssen durch dedizierte Administratorenrollen bewerkstelligt werden, die über separate Zugänge verfügen.

2 Netzwerkeinstellungen und Verbindungswege

2.1 Benötigte IPv4-Adressen:

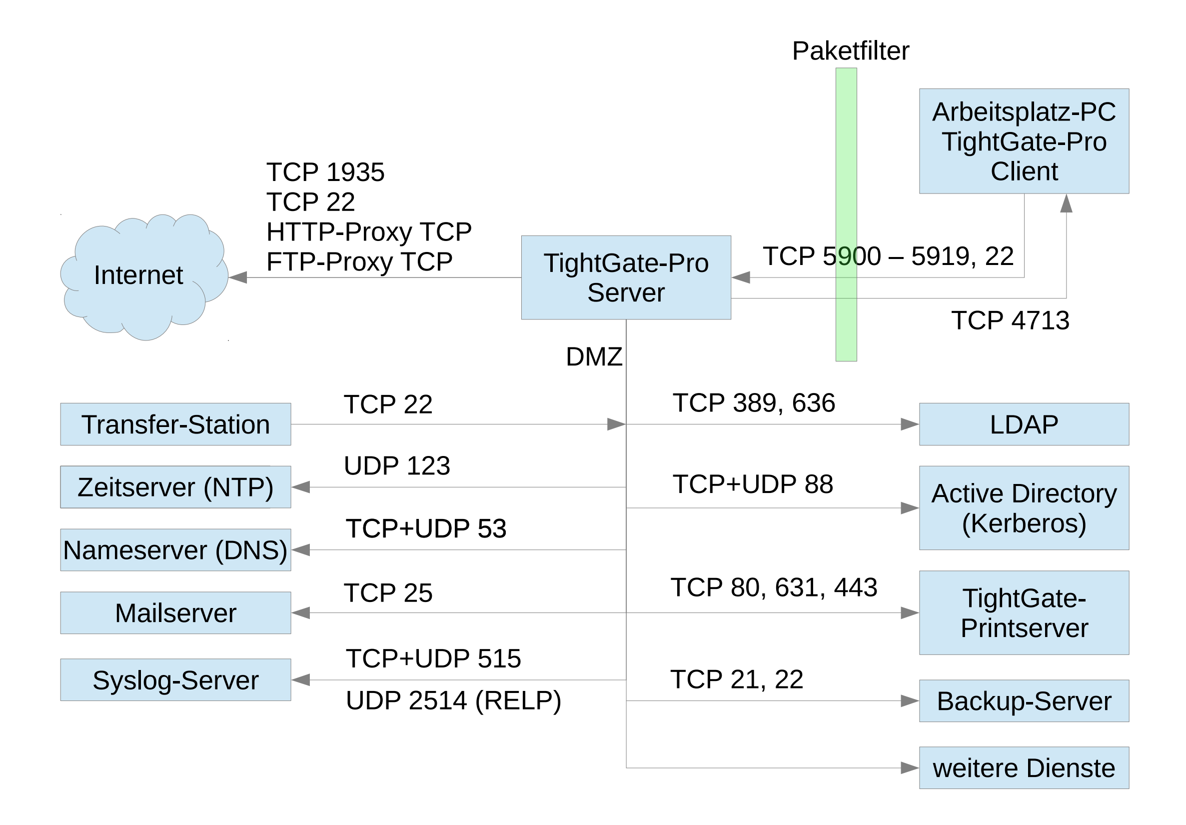
Um die Netzwerkeinrichtung von TightGate®-Pro Server vorzunehmen, werden folgende Informationen zwingend benötigt:

- IPv4-Adresse des Servers /
  bei Rechnerverbünden (Clustersystemen) die des jeweiligen Knotens (Nodes)
- Rechnername und Domäne /
  bei Rechnerverbünden (Clustersystemen) die des jeweiligen Knotens (Nodes)
- Klientennetzwerk(e)
- IPv4-Adresse des Namenservers
- IPv4-Adresse des Gateways
- IPv4-Adresse des NTP-Zeitservers

Ferner werden weitere Informationen benötigt:

- Name bzw. IPv4-Adresse von Proxy, POP3/IMAP- und SMTP-Mailserver,
  Backup-Server
- IPv4-Adressen der / des Printserver/s (CUPS oder LPD)
- IP-Adresse eines CITRIX-Servers, falls Einbindung gewünscht

2.2 Kommunikationsdiagramm



Die nachfolgende Übersicht zeigt die Ports und Protokolle auf, welche benötigt werden, damit TightGate®-Pro im Netzwerk betrieben werden kann. Optional erfolgt die Audioverbindung nicht direkt, sondern über eine zwischengeschaltete Instanz (Socks-Proxy-Server).

Der eingezeichnete Paketfilter ist betreiberseitig zur Verfügung zu stellen und so zu konfigurieren, dass die Pakete des PulseAudio-Systems (Port 4713) nur dann passieren können, wenn zugleich eine VNC-Verbindung zum jeweiligen Arbeitsplatzrechner besteht. Dies wird unabhängig davon durch den zusammen mit dem mit TightGate®-Pro (CC) Version 1.4 Client installierten PulseAudio-Daemon (Audio Sink) sichergestellt. Dieser nimmt nur dann Audio-Streams von TightGate®-Pro (CC) Version 1.4 Server an, wenn der VNC-Klient von TightGate®-Pro (CC) Version 1.4 Client zeitgleich verbunden ist, und auch dann ausschließlich von der IPv4-Adresse der bereits bestehenden Verbindung. Der nach PP 0040 ReCoBS geforderte Paketfilter stellt diese Bedingungen auch im Fall eines Softwarefehlers in TightGate®-Pro (CC) Version 1.4 Client sicher.

Der zusammen mit TightGate®-Pro (CC) Version 1.4 Client installierte PulseAudio-Daemon verfügt über einen reduzierten Funktionsumfang, der nur die unbedingt notwendigen Komponenten umfasst. Potenziell gefahrenträchtige Module, wie beispielsweise eine Mikrofonsteuerung, sind nicht enthalten. Eine entfernte Konfiguration des Daemons ist nicht möglich. Weiterhin wird der Audio-Deamon erst zusammen mit der Benutzersitzung gestartet und nach Beendigung der Session ebenfalls beendet. Diese Charakteristika des Audio-Systems verhindern zusammen mit der angesprochenen Verbindungsselektivität des Klienten, dass der Audio-Kanal eine potenzielle Schwachstelle bildet. Letzterer ist als Teil des funktionsspezifischen Protokolls zwischen TightGate®-Pro Server respektive TightGate®-Pro (CC) Version 1.4 Server und den jeweiligen Klienten anzusehen, das einen wichtigen Baustein des dedizierten ReCoB-Systems darstellt.

Hinweis: In TightGate®-Pro (CC) Version 1.4 Server ist die Audiounterstützung standardmäßig deaktiviert und kann über die Konfigurationsoption ***config > Einstellungen > Audio-Unterstützung*** eingeschaltet werden.

2.3 Firewall-Einstellungen

TightGate®-Pro Server oder TightGate®-Pro (CC) Version 1.4 Server sind grundsätzlich zum Betrieb in einer Demilitarisierten Zone (DMZ) vorgesehen. Es ist sicherzustellen, dass sich Klientenrechner im internen Netzwerk nur über die vorgesehenen Ports mit TightGate®-Pro Server oder TightGate®-Pro (CC) Version 1.4 Server verbinden. Weiterhin ist durch geeignete Firewalls bzw. Paketfilter der direkte Internetzugriff unter Umgehung von TightGate®-Pro Server / TightGate®-Pro (CC) Version 1.4 Server zu unterbinden.

Nicht unbedingt für den ordnungsgemäßen Betrieb von TightGate®-Pro Server erforderliche Verbindungswege sind als „optional“ gekennzeichnet und sollten deaktiviert werden, sofern die hierüber realisierte Funktionalität nicht benötigt wird. Dies betrifft auch die Signalisierung von externen Steuersystemen über SNMP, die sich jedoch auf Statusabfragen beschränkt und ohne Implikation für die Systemsicherheit von TightGate®-Pro Server bleibt.

Hinweis: TightGate®-Pro Server oder TightGate®-Pro (CC) Version 1.4 Server lassen Verbindungen von Klientenrechnern, auf denen TightGate®-Pro Client oder TightGate®-Pro (CC) Version 1.4 Client installiert ist, nur aus eingetragenen Klientennetzen zu. Diese müssen zuvor auf TightGate®-Pro Server oder TightGate®-Pro (CC) Version 1.4 Server konfiguriert werden.

Achtung: Falls die notwendigen Netzwerkports für gewählte Funktionen von TightGate®-Pro nicht zur Verfügung stehen, kann dies zu Einschränkungen insbesondere bei der Audio- beziehungsweise Videowiedergabe führen. Die näheren Hinweise in diesem Administrationshandbuch zu den betreffenden Funktionen von TightGate®-Pro Server sind zu beachten.

2.3.1 Ausgehende Verbindungen zur DMZ, zum Updateserver und zum Internet

Bei UDP-Verbindungen sind zugehörigen UDP-Antwortpakete in Gegenrichtung ebenfalls freizugeben.

Absender	Ziel		Protokoll	Port(s)	Bemerkung
TightGate®-Pro Server	Internet Internet oder ext. Proxy	DMZ oder extern bzw. im Internet	TCP	1935 80, 8080, 443 oder Proxy-Port	Port 1935 wird für bestimmte Sonderdienste im Zusammenhang mit der Videowiedergabe über Adobe Flash benötigt.
TightGate®-Pro Server			TCP	22	Zugriff auf mprivacy-update2.de sowie mprivacy.update.de (Fallback)
TightGate®-Pro Server	Zeitserver		UDP	123	
TightGate®-Pro Server	Nameserver		TCP + UDP	53	
TightGate®-Pro Server	Mailserver		TCP	25	Weitere Freigaben über SMTP: 25 hinaus erforderlich, falls folgende Dienste über TightGate®-Pro Server genutzt werden sollen: POP3: 110 - POP3/SSL: 995 IMAP4: 143 - IMAP4/SSL: 993 LDAP: 389 HTTP: 80 - HTTP/SSL: 443
TightGate®-Pro Server	Active Directory (Kerberos)	DMZ	TCP + UDP	88	Optional[2]
TightGate®-Pro Server	Active Directory Admin-Server		TCP + UDP	750	Optional[2]
TightGate®-Pro Server	LDAP		TCP	389, 636	LDAP / LDAPS – optional[2]
TightGate®-Pro Server	Backup-Server		TCP	21, 22	FTP / SFTP – optional[2]
TightGate®-Pro Server	Cups-Printserver		TCP	80, 631, 443	Optional[2]
TightGate®-Pro Server	Netzwerkdrucker		TCP TCP	515 9100	LPD – optional[2] HP JetDirect – optional[2]
TightGate®-Pro Server	Syslog-Server		TCP + UDP TCP + UDP TCP	kofigurierbar 514 2514	 Standard Syslog Standard RELP

2 Diese Ports sind nur freizugeben, falls die entsprechenden Dienste genutzt werden, d. h. in den Einstelloptionen von TightGate®-Pro Server aktiviert wurden. Nicht benötigte oder nicht gewünschte Funktionen müssen deaktiviert werden, bevor der betreffende Netzwerkport auf Firewalls oder Paketfiltern gesperrt wird.

2.3.2 Verbindungen zum internen Netzwerk (Klientennetz im LAN)

Absender	Ziel	Protokoll	Port(s)	Bemerkung
TightGate®-Pro Client (Arbeitsplatz-PC)	TightGate®-Pro Server	TCP	5900 - 5919	Verbindung ist stets TLS-Verschlüsselt.
TightGate®-Pro Server	Arbeitsplatz-PC	TCP	4713	Umleitung über Socks-Proxy ist möglich. Verbindung ist stets unverschlüsselt!
TightGate®-Pro Client (Arbeitsplatz-PC)	TightGate®-Pro Server	TCP	22	SFTP-Verbindung bei Schleusennutzung, TLS-Verschlüsselt – optional[2,3]

2.3.3 Eingehende Verbindungen zu TightGate®-Pro Server

Absender	Ziel	Protokoll	Port(s)	Bemerkung
Interner DNS-Dienst	TightGate®-Pro Server Clustersystem	UDP	53	Optional[2] Dienst wird nur für TightGate®-Pro-Cluster benötigt – siehe Schaubild
Monitoring-System (Statusabfrage)	TightGate®-Pro Server	UDP	161	SNMP – optional[2]
NRPE-Monitoring (NAGIOS)	TightGate®-Pro Server	TCP + UDP	5666	Optional[2]
Zeitserver	TightGate®-Pro Server	UDP	123	Antworten des Zeitservers.
Netzwerkdrucker	TightGate®-Pro Server	UDO	161	Antworten von Netzwerkdruckern.

2.3.4 Sonstige Verbindungen

Absender	Ziel	Protokoll	Port(s)	Bemerkung
TightGate®-Pro Server	SSH-Klient	TCP	22	Ausgehend, optional[2]
TightGate®-Pro Server	FTP-Klient	TCP	21	Eingehend, optional[2] Zugehörige TCP-Verbindungen aus- und eingehend –
TightGate®-Pro Server	RDP- bzw. CITRIX-Server	TCP UDP	3389, 1494, 80, 443 1604	Ein- und ausgehend, optional[2]

3 Nicht verfügbar bei TightGate®-Pro (CC) Version 1.4.

3 Systemstart und Betriebsmodi

Nach der vorschriftsmäßigen Installation gemäß Installationshandbuch kann TightGate®-Pro Server über den Einschalter an der Frontblende der Serverrechner oder via KVM-Remotekonsole oder über das IPMI-Interface gestartet werden. TightGate®-Pro Server folgt nach dem Einschalten einer festgelegten Hochfahrprozedur. Diese ist so gestaltet, dass sich TightGate®-Pro Server ohne Bedienereingriff automatisch im korrekten und maximal sicheren RSBAC-Betriebsmodus befindet. In diesem Modus sind sämtliche Kontroll- und Sicherheitssysteme von TightGate®-Pro Server standardmäßig aktiviert.

3.1 Startmenü

Falls TightGate®-Pro Server ausnahmsweise in einem anderen Betriebsmodus, abweichend vom RSBAC-Modus, gestartet werden soll, kann dies während der Startphase festgelegt werden. Nach dem Einschalten erscheint für ca.10 Sekunden das Startmenü von TightGate®-Pro Server. Es stehen folgende Wahlmöglichkeiten zur Verfügung:

Startphase (Hochfahrprozedur)		**Hinweise**		
Startmenüpunkt	**Beschreibung**	**C**	**E**	**F**
RSBAC	Regulärer Betriebsmodus von TightGate®-Pro Server. Dieser Betriebsmodus wird automatisch gewählt, wenn während der Einblendzeit des Startmenüs (ca. 10 Sekunden) keine andere der angezeigten Optionen ausgewählt wird. Im RSBAC-Modus sind sämtliche Sicherheits- und Kontrollsysteme von TightGate®-Pro Server aktiviert. TightGate®-Pro Server sollte regulär ausschließlich in diesem Betriebsmodus betrieben werden. Vor einer Umschaltung in andere Betriebsmodi ist die Konsultation des technischen Kundendienstes der m-privacy GmbH dringend angeraten. **Achtung:** Im Fall von TightGate®-Pro (CC) Version 1.4 Server entspricht ausschließlich dieser Betriebsmodus den Anforderungen gem. CC.			
RSBAC-Debug	Betriebsmodus zur Systemanalyse unter speziellen Betriebsbedingungen. Nur in Abstimmung mit dem technischen Kundendienst der m-privacy GmbH zu verwenden. **Hinweis:** Dieser Betriebsmodus ist für den regulären Systembetrieb nicht notwendig. Das Schutz- und Sicherheitsniveau entspricht dem des Modus „RSBAC“, es werden jedoch zahlreiche Diagnosemeldungen ausgegeben.			
Softmode	Betriebsmodus unter Deaktivierung sämtlicher Sicherheits- und Kontrollsysteme von TightGate®-Pro Server. Nur in Abstimmung mit dem technischen Kundendienst der m-privacy GmbH zu verwenden. **Warnung:** Dieser Betriebsmodus ist für den regulären Systembetrieb nicht geeignet. Es sollte unbedingt darauf geachtet werden, dass keine Benutzer mit dem System verbunden sind, während der Softmode aktiviert ist! Die Systemsicherheit kann beeinträchtigt werden, wenn dieser Betriebsmodus zu einem anderen Zweck verwendet wird, als in Abstimmung mit dem technischen Kundendienst der m-privacy GmbH erörtert. **Hinweis:** Bei TightGate®-Pro (CC) Version 1.4 Server ist eine Anmeldung in den Administrationsrollen ***root*** und ***security*** nur im Softmode möglich. Der VNC-Server wird zugleich deaktiviert, eine Anmeldung von Klienten über den TightGate®-Viewer ist im Softmode nicht möglich.			

Startphase (Hochfahrprozedur)		Hinweise		
Startmenüpunkt	**Beschreibung**	**C**	**E**	**F**
Recover	Betriebsmodus zur Systemwiederherstellung bzw. Neuinstallation. Nur in Abstimmung mit dem technischen Kundendienst der m-privacy GmbH zu verwenden. **Warnung:** Dieser Betriebsmodus ist für den regulären Systembetrieb nicht geeignet. Die Systemsicherheit kann beeinträchtigt werden, wenn dieser Betriebsmodus zu einem anderen Zweck verwendet wird, als in Abstimmung mit dem technischen Kundendienst der m-privacy GmbH erörtert.			
Speichertest	Automatisiertes Testverfahren zur Überprüfung des installierten Arbeitsspeichers. Nur in Abstimmung mit dem technischen Kundendienst der m-privacy GmbH zu verwenden. **Hinweis:** In diesem Betriebsmodus erfolgt kein Systembetrieb von TightGate®-Pro Server. Zur Wiederaufnahme des Systembetriebs im RSBAC-Modus ist ein Neustart erforderlich. Im Zuge der Hochfahrprozedur kann ein anderer Betriebsmodus gewählt oder der Speichertest wiederholt werden.			

Warnung: Sobald ein anderer Betriebsmodus als „RSBAC“ gewählt wurde, arbeitet TightGate®-Pro Server nicht mehr CC-konform! Zudem kann die Systemsicherheit, die Sicherheit des internen Netzwerks sowie die der Arbeitsplatzrechner (Klientenrechner) erheblich beeinträchtigt werden! TightGate®-Pro (CC) Version 1.4 Server darf zum Zweck des regulären Systembetriebs nicht in einem anderen Modus gestartet werden als „RSBAC“!

Eigenschaften der Betriebsmodi					
	RSBAC	**RSBAC-Debug**	**Recover**	**Softmode**	**Speichertest**
Benutzeranmeldung möglich	ja	ja	nein	nein	nein
Administrationszugänge freigeschaltet	ja	ja	nein	ja	nein
Netzwerkverbindungen aktiv	ja	ja	nein	ja	nein
RSBAC-Sicherheitssystem aktiv	ja	ja	nein	nein	nein

Nach Ende der Startphase erscheint der Konsolenprompt. Von diesem Augenblick an können sich Administratoren anmelden und das System kann Verbindungsanfragen der Klientenrechner (Arbeitsplatzrechner) verarbeiten.

3.2 Varianten- und Versionsprüfung

Das ReCoB-System TightGate®-Pro ist in zwei Varianten verfügbar. Diese sind TightGate®-Pro für Standardumgebungen (im Folgenden nur als „TightGate®-Pro“ bezeichnet) und TightGate®-Pro (CC) Version 1.4 für CC-konforme Umgebungen. Zur Überprüfung von Variante und Version von TightGate®-Pro bestehen mehrere Optionen:

- Prüfung über die Statusseite von TightGate®-Pro Server beziehungsweise von TightGate®-Pro (CC) Version 1.4 Server. Die Statusseite kann im Browser eines beliebigen, angemeldeten Benutzers mittels ***http://localhost*** aufgerufen werden. Bei Aufruf der Statusseite wird ein Anmeldedialog eingeblendet. Das erforderliche Passwort wird während der Instal-

lation des Systems festgelegt. Im Fall von TightGate®-Pro (CC) Version 1.4 Server erfolgt bei Abweichungen von den CC-konformen Grundeinstellungen zusätzlich ein entsprechender Hinweis.

- Prüfung über einen Administratorenzugang. Die Menüs der Administratorenzugänge tragen in der Kopfzeile eine Kennung hinsichtlich des installierten Systems. Im Fall von TightGate®-Pro (CC) Version 1.4 Server erfolgt bei Abweichungen von den CC-konformen Grundeinstellungen zusätzlich ein entsprechender Hinweis.

3.3 Statusseite

TightGate®-Pro Server verfügt über eine interne Statusseite, die sich über den Browser eines angemeldeten VNC-Benutzers abrufen lässt. Sie vermittelt grundlegende Informationen über das laufende System und die wichtigsten Systemdienste, ohne dass es eines Aufrufs der Administrationsmenüs bedürfte. Die Signalisierung der Systemzustände erfolgt durch Werteanzeige sowie eine augenfällige Rot-/Grün-Kennzeichnung. Nach jedem Update oder Teilupdate des Systems wird das Datum der letzten Aktualisierung auf der Statusseite neu gesetzt.

Die Statusseite kann im Browser mittels ***http://localhost*** aufgerufen werden.

Bei Aufruf der Statusseite wird ein Anmeldedialog eingeblendet. Das erforderliche Passwort wird während der Installation des Systems festgelegt. Es kann nach Anmeldung als Administrator ***config*** unter dem Menüpunkt ***config > Einstellungen > Status: Passwort*** bei Bedarf geändert werden. Nach Eingabe der Benutzerkennung „status“ und des gesetzten Passworts wird die Statusseite angezeigt. Die Darstellung wird alle 120 Sekunden automatisch im Browser geladen, die angezeigten Systemstatistiken werden jedoch nur stündlich aktualisiert.

Achtung: Falls das Passwort manuell gelöscht wird, ist die Statusseite von jedem angemeldeten VNC-Benutzer über den Browser einsehbar!

Die Statusseite informiert auch über die korrekte Funktion des serverseitigen Malware-Scanners, falls ein solcher installiert ist. In diesem Fall wird auch der Aktualisierungszeitpunkt der Schadcode-Definitionsdateien (Virensignaturen) angezeigt. Sollten die Signaturen älter als drei Tage sein, wechselt die Statusanzeige auf Rot. In diesem Fall könnte ein Konfigurationsfehler vorliegen oder der betreffende Updateserver ist nicht erreichbar.

Weiterhin wird auf der Statusseite eine Abweichung von den CC-konformen Einstellungen durch Anzeige des Hinweistextes „Abweichungen von CC, siehe config!“ in der Kopfzeile des Menübildschirms signalisiert. Die Darstellung ist im Sinne einer möglichst hohen Signalwirkung in gelber Schriftfarbe gehalten und erscheint in der rechten oberen Ecke der Statusseite.

Hinweise: Auf der Statusseite können keine Änderungen an den angezeigten Parametern vorgenommen werden. Die Werte dienen nur der Information hinsichtlich grundlegender Betriebszustände. Zur Administration des Systems dienen die Administrationsmenüs und die unterschiedlichen Administrationsrollen. Zur Detailüberwachung des Systembetriebs ist eine Überwachung mittels Nagios anzuraten, zumal für TightGate®-Pro Server zahlreiche systemspezifische Sensoren und Prüfpunkte zusätzlich zu den regulären Funktionen der Nagios-Systemüberwachung verfügbar sind.

3.4 Neuinstallation und Wiederherstellung

Hinweise zur Neuinstallation des Systems bzw. dessen Wiederherstellung im Havariefall können dem Installationshandbuch entnommen werden. Zu beachten sind auch die weiterführenden Hinweise in Kapitel 8 Datensicherung.

Warnung: Der Serverrechner im Vorfeld einer Installation von TightGate®-Pro Server sollte ohne lauffähiges TightGate®-Pro-Betriebssystem mit aktiviertem RSBAC aus Sicherheitsgründen nur in einer Demilitarisierten Zone (DMZ) oder alternativ gänzlich ohne Netzwerkverbindung in Betrieb genommen werden.

3.5 Rücksetzung in einen sicheren Zustand (OE.Reset)

Hinweise zur Rückversetzung von TightGate®-Pro (CC) Version 1.4 Server in einen definierten, als sicher bekannten Ausgangszustand unter Verwendung eines mitgelieferten Installationsmediums können dem Installationshandbuch entnommen werden. Zu beachten sind auch die weiterführenden Hinweise in Kapitel 8 Datensicherung.

Warnung: Der Serverrechner im Vorfeld einer Installation von TightGate®-Pro Server sollte ohne lauffähiges TightGate®-Pro-Betriebssystem mit aktiviertem RSBAC aus Sicherheitsgründen nur in einer Demilitarisierten Zone (DMZ) oder alternativ gänzlich ohne Netzwerkverbindung in Betrieb genommen werden. Nach erfolgter Rücksicherung der Systemkonfiguration nach einem OE.Reset ist der Neustart des Systems unbedingt erforderlich.

4 Konfiguration

Die gesamte Administration von TightGate®-Pro Server erfolgt menügesteuert in deutscher oder englischer Sprache. Die Verwaltung des Schutzsystems über eine Kommandozeile ist nicht möglich. Aus Sicherheitsgründen ist keine Programmschnittstelle (API) zu anderen Systemen implementiert.

4.1 Menügeführte Konfigurationsoberfläche

Die menügeführte Konfiguration wird für sämtliche Administratorzugänge in einem Konsolenfenster aufgerufen. Es stehen mehrere Zugangswege zur Verfügung, die sich durch die folgenden Eigenschaften auszeichnen:

- Der konsolenbasierte Zugriff direkt am Serverrechner ist für alle Administratorzugänge immer möglich.
- Für TightGate®-Pro (CC) Version 1.4 Server ist der Administratorzugang ausschließlich direkt am Serverrechner oder alternativ per KVM-Umschalter möglich.
- Andere Versionen von TightGate®-Pro Server ermöglichen für die regulären Administrationszugänge ***config***, ***maint***, ***update*** und ***backuser*** zusätzlich eine Remote-Verbindung via SSH (TCP-Port 22).
  Hinweis:
  Ist unter ***config > Einstellungen > Wartung und Updates > Ferne Administrator-IP*** keine IPv4-Adresse eingetragen, kann der entsprechende Zugriff per SSH nur aus dem Klientennetz erfolgen. Rechner außerhalb des Klientennetzes, von denen zusätzliche eine Anmeldung in einer der Administratorenrollen erfolgen soll, sind mit ihrer IPv4-Adresse einzutragen. Bei TightGate®-Pro (CC) Version 1.4 Server ist dieser Menüpunkt mit ***Nagios / Storage IP*** bezeichnet, da die Administration per SSH bis auf die im folgendemn Punkt beschriebenen Ausnahmen ausgeschlossen ist.
- Für die Administratoren ***root*** und ***security*** ist zur Anmeldung an TightGate®-Pro Server zusätzlich eine Freischaltung durch den Administrator ***maint*** im jeweiligen Menü erforderlich, um den SSH-Zugang nutzen zu können. Zusätzlich besteht eine zeitliche Beschränkung; nach Ablauf von einer Stunde wird die Anmeldeoption per SSH automatisch deaktiviert und muss im Bedarfsfall erneut freigegeben werden. Im Fall von TightGate®-Pro (CC) Version 1.4 Server ist die Anmeldung der Administratoren ***root*** und ***security*** per SSH nur dann möglich, wenn der Server im sogenannten Softmode gestartet wurde und eine IPv4-Adresse eines verwaltungsberechtigten Rechners außerhalb des Klientennetzes (!) unter ***config > Einstellungen > Wartung und Updates > Nagios / Storage IP*** hinterlegt wurde.

Wir empfehlen das lizenzkostenfrei verfügbare Terminalprogramm „puTTY“ zur Verbindung mit dem ReCoBS-Server. Eine webbasierte Administration von TightGate®-Pro Server ist aus Sicherheitsgründen nicht möglich.

In sämtlichen Menüs, die für die Wartungs- und Konfigurationsaufgaben zur Verfügung stehen, können einzelne Menüpunkte jeweils mit den Pfeiltasten (Cursortasten) AUF und AB ausgewählt werden. Mit den Pfeiltasten LINKS und RECHTS kann zwischen <OK> und <Abbruch> gewählt werden. <OK> wählt die jeweilige Option aus, <Abbruch> bewirkt einen Rücksprung auf die darüberliegende Menüebene. Die Tastenkombination ALT+C und die Taste ESC sind gleichbedeutend mit <Abbruch>. Im Hauptmenü wird die Benutzeroberfläche mit dem zuoberst stehenden Menüpunkt geschlossen, es erfolgt die Anzeige des Konsolenfensters oder bei einer SSH-Verbindung der Abbruch der Verbindung.

Die ersten Schritte zur Installation und Inbetriebnahme werden im Installationshandbuch zusammenfassend erläutert (AGD_PRE).

Hinweis: Nachfolgend werden alle möglichen Menüoptionen zur Konfiguration von TightGate®-Pro Server thematisch gegliedert und unabhängig von der Reihenfolge ihrer Anwendbarkeit aufgeführt. Zur leichteren Orientierung befindet sich der Navigationspfad vom Hauptmenü bis zum jeweiligen Untermenü in Kopf einer jeden Optionstabelle. Insbesondere in der Beschreibung der Hauptmenüs werden

nicht alle Einstelloptionen der jeweiligen Untermenüs erschöpfend erläutert. Die zugehörigen Informationen finden sich jedoch an anderer Stelle dieser Dokumentation.

Achtung: In den meisten Fällen sind Auswahl- und Einstellmöglichkeiten nur bestimmten Administratoren zugänglich. So können einige Optionen beispielsweise nur durch den Administrator ***maint***, andere nur durch den Administrator ***config*** gewählt werden.

4.2 Signalisierung von Konfigurationsabweichungen

Die CC-Konformität von TightGate®-Pro (CC) Version 1.4 Server ist nur bei durchgehend CC-konformen Konfigurationseinstellungen gegeben. Um das System nicht irrtümlich mit abweichenden und damit nicht CC-konformen Einstellungen zu betreiben, werden abweichende Einstellungen in den Administrationsmenüs von TightGate®-Pro (CC) Version 1.4 Server auffällig gekennzeichnet.

4.2.1 Betroffene Einstelloptionen

Folgende Einstelloptionen des Administrators ***config*** unter ***config > Einstellungen*** müssen in der für TightGate®-Pro (CC) Version 1.4 Server geltenden Vorgabe beibehalten werden, um die CC-Konformität des Gesamtsystems nicht zu gefährden:

Einstelloption	Vorgabewert	Alternativwert(e)
Dateischleuse: Erlauben	nein	ja
Magische URLs	nein	ja
Benutzer-Shell erlauben	nein	ja
Fernadministration	nein	ja

4.2.2 Signalisierung in den Administrationsmenüs

Abweichungen von CC-konformen Konfigurationseinstellungen werden im Administrationsmenü des Administrators ***config*** durch Anzeige des Hinweistextes „CC-Abweichung!“ in der Kopfzeile des Menübildschirms signalisiert. Die Darstellung ist in gelber Schriftfarbe gehalten und erscheint auf gleicher Höhe wie der Hinweis zum Speichern oder Anwenden von Änderungen. Wurden Updates eingespielt, erscheint in der Titelzeile der gelb dargestellte Hinweis „+Updates“. Ein weiterer Hinweis bei dem jeweiligen Menüpunkt stellt Abweichung und Vorgabe gegenüber. Der Hintergrund des Menübildschirms wechselt bei Abweichungen von CC-konformen Vorgaben von Blau nach Gelb, solange diese Abweichungen bestehen.

4.2.3 Signalisierung auf der Statusseite

Auch auf der Statusseite von TightGate®-Pro (CC) Version 1.4 Server, welche im Browser eines angemeldeten Benutzers mittels ***http://localhost*** aufgerufen werden kann, wird eine Abweichung von den CC-konformen Einstellungen durch Anzeige des Hinweistextes „Abweichungen von CC, siehe config!“ in der Kopfzeile des Menübildschirms signalisiert. Die Darstellung ist im Sinne einer möglichst hohen Signalwirkung in gelber Schriftfarbe gehalten und erscheint in der rechten oberen Ecke der Statusseite.

4.3 Spracheinstellungen

TightGate®-Pro Server unterstützt Mehrsprachigkeit bei der Administration und für die VNC-Benutzeroberfläche. Die Spracheinstellungen werden als Administrator ***config*** im Hauptmenü unter Spracheinstellungen vorgenommen.

Hinweis: Mehrsprachigkeit bei der Eingabe landesspezifischer Sonderzeichen wird in TightGate®-Pro Server mittels des Frameworks „IBus“ (Intelligent Input Bus) realisiert. IBus kann als Administrator ***update*** eingerichtet und dann als angemeldeter VNC-Benutzer in allen Eingabemasken des Systems und im Webbrowser verwendet werden.

config > Sprach-Einstellungen		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Menüsprache	Auswahl der Sprache, die für die Administration des TightGate®-Pro Server gelten soll. Diese Einstellung wirkt sich auf alle Administrationsmenüs gleichermaßen aus und wird erst nach einer Neuanmeldung wirksam. Es stehen derzeit die Sprachen Deutsch und Englisch zur Verfügung, weitere Sprachen können auf Anfrage bereitgestellt werden.		**E1**	**F0**
Benutzersprache	Auswahl der Standardsprache für die VNC-Benutzer (Anwender an den Arbeitsplatzrechnern). Die Einstellungen werden nach Verlassen des Untermenüs sofort wirksam. Bei bereits angemeldeten Benutzern wirken sich die Einstellungen bei der nächsten Anmeldung an TightGate®-Pro Server aus. Für die VNC-Benutzer sind alle verbreiteten Sprachen verfügbar. Unter Umständen müssen die betreffenden Sprachpakete jedoch nachträglich installiert werden. Diese Aufgabe übernimmt der technische Kundendienst der m-privacy GmbH im Rahmen abzuschließender Verträge zur Softwarepflege. **Hinweis:** Wird die Benutzersprache auf Französisch geändert, werden auch die von diesem Zeitpunkt an generierten Konfigurationsdateien für die Dateischleuse im Zusammenhang mit einer Anmeldung per SSO in der jeweiligen Sprache erzeugt.		**E1**	**F0**

4.4 Netzwerk-Konfiguration (*config*)

Nach Anmeldung an der Konsole als Administrator ***config*** ist das Menü zur Konfiguration der Netzwerkeinstellungen über das Untermenü Einstellungen zugänglich.

Hinweis: Die mit einem * markierten Menüpunkte gelten bei einem Cluster-System für den gesamten Cluster, müssen also nur auf einem System eingestellt werden. Die Markierung ist auch im Menü auf dem System sichtbar.

4.4.1 Einstellungen für TightGate®-Pro Server

config > Einstellungen		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Zurück	Rückkehr zum Hauptmenü.		**E0**	
Speichern	Konfigurationsdatei wird abgespeichert, Einstellungen werden noch nicht wirksam.		**E0**	**F0**
Voll Anwenden (Warmstart)*	Übernahme und Aktivierung der vorgenommenen Einstellungen im System. Relevante Dienste werden neu gestartet. **Warnung:** Da Dienste neu gestartet und Netzwerkverbindungen zurückgesetzt werden, kann es zu Betriebsunterbrechungen und Datenverlust bei angemeldeten Benutzern kommen. Diese Funktion sollte daher im laufenden Produktivbetrieb nicht ausgelöst werden. **Hinweis:** Diese Funktion sollte nur bei zwingender Notwendigkeit ausgelöst werden. Generell genügt in aller Regel ***Sanft Anwenden*** zur Übernahme systemnaher Einstellungen.		**E2**	**F0**
Sanft Anwenden*	Übernahme und Aktivierung der vorgenommenen Einstellungen im System. Bestehende Verbindungen zu den Arbeitsplatzstationen und zu anderen Netzwerkressourcen werden nach Möglichkeit nicht getrennt. Im Rechnerverbund wird der Befehl zum ***Sanft Anwenden*** auf alle Knoten (Nodes) verteilt und spätestens nach 5 Minuten automatisch ausgeführt. Falls Umstände vorliegen, die ***Sanft Anwenden*** verhindern, unterbleibt dieser Vorgang so lange, bis ***Sanft Anwenden*** wieder möglich ist. Ist etwa der Administrator ***config*** noch am System angemeldet, ist ***Sanft Anwenden*** nicht möglich. **Warnung:** Kann ***Sanft Anwenden*** nur auf einigen, jedoch nicht auf allen Knoten (Nodes) eines Rechnerverbunds ausgeführt werden, kann dies zu instabilem Systembetrieb führen! Eine Warnmeldung im ***config***-Menü weist auf die Notwendigkeit zum ***Sanft Anwenden*** hin. **Hinweis:** ***Sanft Anwenden*** ist das gebräuchliche Verfahren zur Übernahme systemnaher Einstellungen.		**E0**	**F0**
Übersicht	Anzeige einer Übersicht sämtlicher Netzwerkeinstellungen von TightGate®-Pro Server.		**E0**	**F0**
Mailversand (unverschlüsselt)	Versand der Konfigurationseinstellungen per E-Mail. Es kann eine beliebige E-Mail-Adresse angegeben werden, beispielsweise die eines externen Dienstleisters. Voraussetzung für den Versand von E-Mails über das System von TightGate®-Pro Server ist die ordnungsgemäße Konfiguration der E-Mail-Einstellungen im jeweiligen Systemmenü.		**E3**	**F0** **F3**

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
	Achtung: Die im Anschluss an diese Tabelle aufgeführten Voraussetzungen zum E-Mail-Versand aus TightGate®-Pro Server sind unbedingt zu beachten! **Hinweis:** Die Daten werden unverschlüsselt übertragen.			
Versand an Support	Versand der Konfigurationseinstellungen per E-Mail an den technischen Kundendienst der m-privacy GmbH. Voraussetzung für den Versand von E-Mails über das System von TightGate®-Pro Server ist die ordnungsgemäße Konfiguration der E-Mail-Einstellungen im jeweiligen Systemmenü. **Achtung:** Die im Anschluss an diese Tabelle aufgeführten Voraussetzungen zum E-Mail-Versand aus TightGate®-Pro Server sind unbedingt zu beachten! **Hinweis:** Die Daten werden verschlüsselt übertragen.		**E2**	**F0**
Wiederherstellen	Rücksicherung der Konfiguration von einem USB-Datenträger oder aus einer lokalen Sicherung. Es kann ein Datenträger ausgewählt werden. Für nähere Informationen zur Datensicherung und Wiederherstellung vgl. Kapitel 9 auf Seite 101ff.		**E1**	**F0**
Rechnername	Bezeichnung des TightGate®-Pro Servers, kann entsprechend der Zielumgebung gewählt werden. Bei Clustersystemen endet der Name grundsätzlich mit der laufenden Nummer im Cluster.		**E4**	
Domäne*	Netzwerkdomäne des TightGate®-Pro Servers, kann entsprechend der Zielumgebung beliebig gewählt werden.		**E4**	
SSL-Name im Zertifikat*	DNS-Systemname im SSL-Zertifikat, den Benutzer verwenden. Bei Clustersystemen muss hier der Domain-Name des TightGate®-Pro Clusters eingetragen werden.		**E4**	**F8**
Domäne Mailversand*	Sendedomäne für Systemnachrichten.		**E4**	
Empfänger Systemnachrichten*	E-Mail-Konto, das Systemnachrichten von TightGate®-Pro Server erhalten soll. **Achtung:** Die im Anschluss an diese Tabelle aufgeführten Voraussetzungen zum E-Mail-Versand aus TightGate®-Pro Server sind unbedingt zu beachten!		**E3**	
Netzwerk-Schnittstellen	Konfiguration der in TightGate®-Pro Server vorhandenen Netzwerkschnittstellen. Die Einstellungen sind entsprechend der Einsatzumgebung vorzunehmen, sofern keine werkseitige Voreinstellung vorhanden ist oder diese geändert werden soll. **Hinweis:** Bei Fragen zur Konfiguration der Netzwerkschnittstellen ist die Konsultation des technischen Kundendienstes der m-privacy GmbH empfehlenswert.		**E1** **E2** **E5**	**F8**
Nameserver*	IPv4-Adresse eines Nameservers (DNS) zur Auflösung von IPv4-Adressen. Es können bis zu 25 Nameserver referenziert werden. Sie werden erforderlichenfalls in der Reihenfolge der Einträge angefragt, falls einzelne Server nicht erreichbar sein sollten.		**E4**	**F5**
Lokale Domänen-Namensserver*	Festlegung der lokalen Domänen und der zugehörigen Nameserver. **Hinweis:** Diese Einstellung ist insbesondere bei AD-Anbindung wichtig, wenn der AD-Server keine DNS-Auflösung ins Internet ausführen kann.		**E4**	**F5**

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
	Achtung: In der Regel muss auch die Rückauflösung (IPv4-Adresse → DNS-Name) explizit angegeben werden.			
Zeitserver*	IPv4-Adresse eines Zeitservers zum Bezug der Systemzeit. Es können bis zu 25 Zeitserver referenziert werden. Diese werden erforderlichenfalls in der Reihenfolge der Einträge angefragt, falls einzelne Server nicht erreichbar sein sollten. **Warnung:** Insbesondere in Clustersystemen ist die korrekte Systemzeit über alle Nodes von großer Bedeutung. Zeitunterschiede zwischen den Rechnern eines Verbunds können zu Betriebsstörungen führen. Daher ist unbedingt darauf zu achten, dass zumindest ein Zeitserver stets erreichbar ist. Es empfiehlt sich, hinreichend viele Alternativen als Ausfallsicherung einzutragen.		**E5**	**F5**
System-Mail-SMTP*	IPv4-Adresse des Standardservers für den E-Mail-Versand.		**E5**	**F5**
LPD-Druckserver*	Die LPD-Druckserver werden in der Form [IP-Adresse/Valid Bits] in CIDR-Notation referenziert. Beispiel: 192.168.1.0/24 für Druckserver aus dem Bereich 192.168.1.1 - 192.168.1.254. Es können bis zu 25 LPD-Druckserver (Netzwerke) referenziert werden.		**E5**	**F5**
CUPS-Druckserver: IP*	IPv4-Adresse des CUPS-Servers (Netzwerk). Es können bis zu 25 CUPS-Printserver (in unterschiedlichen Netzwerken) referenziert werden.		**E5**	**F5**

Achtung: TightGate®-Pro Server kann bei Bedarf System- und Supportinformationen an bestimmte E-Mail-Adressen versenden. Der E-Mail-Versand aus TightGate®-Pro Server setzt jedoch eine korrekte Konfiguration aller relevanten Parameter zwingend voraus. Insbesondere ist darauf zu achten, dass

- in der Menüoption „Domäne E-Mailversand“ eine von einem erreichbaren, externen DNS-Server korrekt auflösbare Domäne eingetragen ist, sowie
- in der Menüoption „Empfänger Systemnachrichten“ eine gültige E-Mail-Adresse eingetragen ist,
- in der Menüoption „System-Mail-SMTP“ ein korrekter Wert hinterlegt ist.

Hinweis: Die nachfolgenden Einstellungen für die Authentifizierung über LDAP, AD oder Kerberos sind nur durch geschultes Personal vorzunehmen. Wegen der Komplexität der jeweiligen Anmeldemethoden wird nachdrücklich empfohlen, diese Einstellungen in Zusammenarbeit mit dem technischen Kundendienst der m-privacy GmbH vorzunehmen.

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Backup-Server*	IPv4-Adressen von Backup-Servern, auf die Datensicherungsdateien ausgelagert werden sollen. Es sind bis zu 25 Einträge möglich, die vom Administrator ***config*** vorgegeben werden können. Die endgültige Auswahl, auf welchem Server die Sicherung ausgelagert wird, trifft der Administrator ***backuser***. Für nähere Informationen zur Datensicherung und Wiederherstellung vgl. Kapitel 9 auf Seite 101ff.		**E5**	**F5**

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Malware-Scanner*	Auswahl des gewünschten Malware-Scanners zur Überwachung der Dateischleuse. Es werden nur solche Malware-Scanner angezeigt, die im System installiert sind. Nähere Hinweise zur Installation der Malware-Scanners F-Prot und ESET finden sich im Kapitel 7: Konfiguration der Dateischleuse. **Hinweis:** Eine Auswahl ist nur möglich, wenn ein entsprechendes Produkt installiert ist.		**E1**	
Weitere Einstelloptionen zum Malware-Scanner	Die folgenden Einstelloptionen sind je nach installiertem Malware-Scanner unterschiedlich. Nähere Hinweise zur Installation des Malware-Scanners finden sich im Kapitel 7: Konfiguration der Dateischleuse.			
Malware-Scanner starten *	Ein- bzw. Abschalten des On-Access-Malware-Scanners. Nähere Hinweise zur Installation des Malware-Scanners finden sich im Kapitel 7: Konfiguration der Dateischleuse.		**E1**	
Aktion STRG-ALT-Entf*	Die Tastenkombination kann genutzt werden, um das System neu zu starten oder um es korrekt herunterzufahren. Alternativ kann diese Tastenkombination ignoriert werden, um keine der vorgenannten Aktionen irrtümlich auszulösen.		**E1**	
Authentisierung*	Auswahl der Authentisierungsmethode für Benutzer. Wird die in TightGate®-Pro Server integrierte Benutzerverwaltung verwendet, sollte im zugehörigen Untermenü in jedem Fall „RSBAC-Lokal“ ausgewählt sein.		**E1** **E4** **E5**	**F5** **F8**
Pseudonymisierung*	TightGate®-Pro Server bietet umfangreiche Protokollierungsmöglichkeiten. Eine Festlegung, ob Benutzernamen im Klartext oder pseudonymisiert festgehalten werden sollen, ist hier möglich.		**E1**	

4.4.2 Einstellungen für Klientenrechner

Nachfolgende Einstellungen haben unmittelbare Auswirkungen auf die Benutzersitzungen bzw. die Arbeitsplatzrechner, sobald sich diese mit TightGate®-Pro Server verbinden. Letztere werden als Klientenrechner oder Klienten bezeichnet.

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Browser-Startseite*	Startseite, welche bei neuen Benutzern im Internetbrowser voreingestellt wird.		**E4**	

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
HTTP-Proxy*	IPv4-Adresse der HTTP-Proxy-Server, über die alle HTTP-Zugriffe in das Internet geleitet werden. Der verwendete Port muss für alle eingetragenen HTTP-Proxy-Server gleich sein und wird in einer gesonderten Menüoption festgelegt. Werden mehrere Server eingetragen, werden diese wahlweise per Rundlauf-Verfahren (Round Robin) oder in einer bestimmten Reihenfolge automatisch angesprochen. Dabei werden die Zugriffe nach Zugriffsgeschwindigkeit gewichtet, nicht erreichbare Server werden automatisch übersprungen. **Achtung:** In den meisten Fällen gibt es nur Server im Netzwerk, die mit expliziter IPv4-Adresse an dieser Stelle einzutragen sind. Für den Ausnahmefall, in dem hier auflösbare DNS-Namen referenziert werden, muss das betreffende Netzwerk unbedingt im Menüpunkt HTTP-Proxy-Netz genau spezifiziert werden und ein DNS-Server muss eingetragen sein, der den Proxy-Namen auflösen kann. Andernfalls ist eine korrekte Verbindung zu den jeweiligen Proxyservern nicht möglich.		**E5**	**F5**
HTTP-Proxy-Reihenfolge*	Falls mehrere Proxy-Server eingetragen wurden, kann mit dieser Option das Auswahlverfahren festgelegt werden. Es steht das Rundlauf-Verfahren (Round-Robin) und die Ansprache nach bestimmter Reihenfolge zur Verfügung. **Hinweis:** Wird nur ein Proxy-Server eingetragen, wird diese Menüoption nicht angezeigt.		**E1**	
HTTP-Proxy-Port*	Angabe des Ports, der zum Kontakt mit den eingetragenen HTTP-Proxy-Servern zu verwenden ist. Muss für alle referenzierten HTTP-Proxy-Server gleich sein.		**E6**	**F6**
HTTP-Proxy-Netz*	Falls ein auflösbarer DNS-Name als Proxyserver eingetragen wird, benötigt das System unbedingt die Information über die IPv4-Adressen, die sich dahinter verbergen. Die IPv4-Adresse ist in CIDR-Notation anzugeben.		**E5**	**F5**
FTP-Proxy*	IPv4-Adresse der FTP-Proxy-Server, über die alle FTP-Zugriffe in das Internet geleitet werden. Der verwendete Port muss für alle eingetragenen FTP-Proxy-Server gleich sein und wird in einer gesonderten Menüoption festgelegt. Die eingetragenen Server werden per Rundlauf-Verfahren (Round Robin) automatisch angesprochen, dabei werden die Zugriffe nach Zugriffsgeschwindigkeit gewichtet. **Achtung:** In den meisten Fällen gibt es nur Server im Netzwerk, die mit expliziter IPv4-Adresse an dieser Stelle einzutragen sind. Für den Ausnahmefall, in dem hier auflösbare DNS-Namen referenziert werden, muss das betreffende Netzwerk unbedingt im folgenden Menüpunkt genau spezifiziert werden und ein DNS-Server muss eingetragen sein, der den Proxy-Namen auflösen kann. Andernfalls ist eine korrekte Verbindung zu den jeweiligen Proxyservern nicht möglich.		**E5**	**F5**
FTP-Proxy-Port*	Angabe des Ports, der zum Kontakt mit den eingetragenen FTP-Proxy-Servern zu verwenden ist. Muss für alle referenzierten FTP-Proxy-Server gleich sein.		**E6**	**F6**

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
FTP Proxy-Netz*	Falls ein auflösbarer DNS-Name als Proxyserver eingetragen wird, benötigt das System unbedingt die Information über die IPv4-Adressen, die sich dahinter verbergen. Die IPv4-Adresse ist in CIDR-Notation anzugeben.		**E5**	**F5**
Proxy ist ein Squid*	Ist diese Menüoption aktiv, werden alle Proxy-Server mit dem schnelleren ICP-Protokoll auf UDP-Port 3130 angesprochen. **Achtung:** Damit die Verbindung zu den Proxy-Servern in diesem Fall funktioniert, muss der UDP-Port 3130 auf allen Paketfiltern und Firewalls zwischen TightGate®-Pro Server und Proxy-Server in beide Richtungen freigeschaltet sein. Andernfalls wird der Proxy-Server als ausgefallen detektiert.		**E1**	
Proxy-Ausnahmen*	IPv4-Adressen oder URLs von Websites, die nicht über den externen Proxy geleitet werden sollen. Diese Angabe wirkt sich als Vorkonfiguration für den Browser aus, der auf TightGate®-Pro Server ausgeführt wird. **Achtung:** Sind in der Menüoption *Proxy-Ausnahmen* Eintragungen erfolgt, müssen diese auch unter *HTTP-Server* eingetragen werden.		**E5**	**F5**
Proxy-Filter*	Einstellungen zur Inhaltsfilterung über einen zusätzlichen internen Proxyserver.		**E1** **E4** **E6**	**F8**
Proxy-Protokollierung*	Festlegung, ob ein anonymes oder mit Kennungen versehenen Proxy-Protokoll erstellt werden soll. Die verwendeten Kennungen können entsprechend der Option „Pseudonyme verwenden“ entweder im Klartext (Benutzername) oder als Pseudonym gespeichert werden. Alternativ kann auf ein Proxy-Protokoll ganz verzichtet werden.Die Log-Daten werden in die Datei access.log des Proxyservers geschrieben.		**E1**	
Proxy-Protokoll-Lebensdauer*	Anzahl der Tage, die das Proxy-Protokoll (access.log) zur Revision beim Benutzer „***revision***“ gespeichert bleibt. Nach Ablauf der Speicherdauer werden die Protokoll-Dateien gelöscht und können nicht rekonstruiert werden. Wird hier 0 eingetragen, findet keine Protokollierung statt.		**E6**	**F6**
Socks-Proxy für Audio*	Einstellung, ob das Audio-Protokoll direkt zum Klientenrechner durchgeleitet werden soll oder ob ein Socks-Proxy vorgeschaltet ist.		**E5**	**F5**
Zwangs-Proxy für Plug-ins	Einstellung, ob alle Browser-Plug-ins, die mit dem Internet Kontakt aufnehmen, zwangsweise über den HTTP-Proxy geleitet werden sollen. Vorgabewert ist „Nein“, d.h. Browser-Plug-ins dürfen eigene Verbindungen in das Internet aufbauen.			
Mail-Einstellungen*	Alle relevanten Einstellungen zur E-Mail-Funktionalität sind der Übersichtlichkeit halber unter diesem Menüpunkt zusammengefasst. Darunter fallen Server-Einstellungen für POP3/IMAP, SMTP sowie die Auswahl des E-Mail-Programms für die Klienten.		**E4** **E5**	**F5**

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
SSH-Server*	IPv4-Adressen der SSH-Server, auf die über TightGate®-Pro Server zugegriffen werden kann. Die Server sind jeweils in CIDR-Notation [IP-Adresse/valid Bits] anzugeben. Es sind maximal 25 SSH-Server (bzw. Netzwerke) erlaubt. Der Dateimanager „pcmanfm“ der neuen LXDE-Oberfläche unterstützt den direkten Zugriff über URLs mit „sftp://...“.		**E5**	**F5**
FTP-Server*	IPv4-Adressen der FTP-Server, auf die über TightGate®-Pro direkt ohne Proxy zugegriffen werden kann. Soll z. B. über TightGate®-Pro eine Website per FTP-Upload gepflegt werden, so muss hier die IPv4-Adresse des betreffenden FTP-fähigen Servers (Webspace) eingetragen werden. Die Server sind jeweils in der CIDR-Notation [IP-Adresse/valid Bits] anzugeben. Es sind maximal 25 FTP-Server (bzw. Netzwerke) erlaubt.		**E5**	**F5**
HTTP-Server*	IPv4-Adressen der HTTP-Server, auf die über TightGate®-Pro direkt ohne Proxy zugegriffen werden kann. Die Server sind in der Form [IP-Adresse/valid Bits] anzugeben. Es sind maximal 25 HTTP-Server (bzw. Netzwerke) erlaubt. **Achtung:** Sind in der Menüoption *Proxy-Ausnahmen* Eintragungen erfolgt, müssen diese auch hier vorgenommen werden.		**E5**	**F5**
RDP/Citrix-Server*	IPv4 Adresse(n) von Citrix- oder Windows-Servern, auf die vom ReCoB-System direkt zugegriffen werden kann. Ein entsprechendes Klienten-Programm stellt m-privacy auf Anfrage im System zur Verfügung. Die Benutzung wird im Benutzer-Handbuch unter Remote Desktop für Verbindungen zu CITRIX- und Windows-Servern beschrieben.		**E5**	**F5**
Syslog-Server*	IPv4-Adressen der Syslog-Server, auf die das TightGate®-Pro-System sein System-Log zusätzlich zur internen Speicherung senden soll. Die Server sind jeweils als IP-Adresse anzugeben. Es sind maximal 25 Server erlaubt. Der Versand erfolgt per UDP auf Port 514 mit fortlaufender Zeilennummer.		**E5**	**F5**
Syslog-Server-Typ*	Art des Syslog-Servers.		**E1**	
Syslog-Server-Port*	Port, über den der Syslog-Server erreichbar ist.		**E6**	**F6**

4.4.3 Systemweite Dienstvorgaben

config > Einstellungen		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Klienten-Netzwerke*	IPv4-Adressen der Netzwerke, die sich mit dem TightGate®-Pro Server verbinden dürfen. Der Zugriff durch TightGate®-Pro Server auf die Klienten-Netzwerke ist grundsätzlich verboten, wenn er nicht durch eine andere Einstellung explizit erlaubt wurde. Sofern für das Klienten-Netzwerk ein spezielles Gateway notwendig ist, so ist dies direkt mit anzugeben. Die Klienten-Netzwerke sind jeweils in der Form [IP-Adresse/valid Bits/gateway] anzugeben. Es sind maximal 25 Klienten-Netzwerke erlaubt. **Warnung:** Das Klienten-Netzwerk darf nicht im Adressbereich 0.0.0.0 mit Valid Bits 0 liegen, da dann kein normaler Internetzugriff möglich ist.		**E5**	**F5**
Privilegierte Klienten*	IPv4-Adressen von Arbeitsplatzstationen, die privilegierten Zugang zu TightGate®-Pro Server erhalten sollen. Alternativ können Netzwerke in CIDR-Notation angegeben werden. In diesem Fall sind alle Klienten privilegiert, deren Arbeitsplatzrechner eine IPv4-Adresse in einem der referenzierten Netzwerke trägt. **Hinweis:** Privilegierte Klienten können auch anhand der Benutzerkennung eingerichtet werden. Dies geschieht in der Benutzerverwaltung als Administrator ***maint***. **Hinweis:** TightGate®-Pro Server unterscheidet zwei Grenzen, bis zu denen Benutzeranmeldungen zugelassen werden. Diese werden in der Lizenz zu TightGate®-Pro Server hinterlegt und sind ausschließlich durch den technischen Kundendienst der m-privacy GmbH veränderbar. Die erste Grenze bezeichnet die Zahl regulärer Benutzer, die zweite Grenze bezeichnet die Zahl der privilegierten Benutzer. Sobald die Zahl zulässiger regulärer Nutzer erreicht ist, werden nur noch privilegierte Nutzer zugelassen - vorausgesetzt, deren Zahl ist noch nicht erreicht. Nach Ausschöpfung der zweiten Grenze wird jeder weitere Verbindungsversuch eines Klienten an TightGate®-Pro Server mit einer entsprechenden Fehlermeldung abgewiesen. Privilegierte Klienten werden nicht nur entsprechend eines gesonderten Kontingents zugelassen, sondern darüber hinaus mit einem größeren Anteil an Arbeits- und Massenspeicher sowie CPU-Zeit auf TightGate®-Pro Server ausgestattet.		**E5**	**F5**
Gefiltertes Web: Vorgabe*	Festlegung des Verhaltens bei der Anlage neuer Benutzer. Neue Benutzer können standardmäßig mit gefiltertem oder mit ungefiltertem Webzugang versehen werden. **Hinweis:** Diese Einstellung ist nur beim Anlegen neuer Benutzer relevant; der betreffende Parameter kann später nutzerindividuell oder gruppenspezifisch beliebig geändert werden.		**E1**	

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Audio pro Benutzer: Vorgabe*	Festlegung des Verhaltens bei der Anlage neuer Benutzer. Neue Benutzer können standardmäßig mit der Möglichkeit zur Wiedergabe von Audiosignalen ausgestattet werden. Weiterhin kann die Audiowiedergabe unter dem Vorbehalt eines positiven Tests freigegeben werden. Verläuft der Test negativ, bleibt die Audiowiedergabe abgeschaltet. **Achtung:** Wird die Audio-Wiedergabe eingeschaltet, ist dann jedoch aufgrund weiterer Randbedingungen im Netzwerk nicht möglich, kommt es zu starken Beeinträchtigungen der Videowiedergabe. Im Zweifelsfall sollte die Einstellung „Testen“ aktiviert oder die Audiowiedergabe bewusst abgeschaltet werden. **Hinweis:** Diese Einstellung ist nur beim Anlegen neuer Benutzer relevant; der betreffende Parameter kann später nutzerindividuell oder gruppenspezifisch beliebig geändert werden.		**E1**	
Dateischleuse: Erlauben*	Die Verwendung der Dateischleuse durch Benutzer kann systemweit erlaubt oder verboten werden. Der dedizierte Transferbenutzer ***transfer*** hat immer Zugriff sofern er sich aus dem Klienten-Netzwerk oder dem Administrations- oder Shared-Storage-Netzwerk anmeldet. **Hinweis:** Wenn die Dateischleuse an dieser Stelle deaktiviert wird, sind die beiden folgenden Menüpunkte zur Dateischleuse ausgeblendet. Die Dateischleuse ist in TightGate®-Pro (CC) Server standardmäßig deaktiviert.			
Dateischleuse: Vorgabe* **Hinweis:** Dieser Menüpunkt ist nur dann verfügbar, wenn die Nutzung der Dateischleuse nicht deaktiviert wurde.	Legt fest, ob neue Benutzer per Voreinstellung berechtigt sind, Daten aus TightGate®-Pro Server mittels der Dateischleuse in das interne Netz oder umgekehrt zu transferieren. **Hinweis:** Diese Einstellung ist nur beim Anlegen neuer Benutzer relevant; der betreffende Parameter kann später nutzerindividuell oder gruppenspezifisch beliebig geändert werden.	**nc**	**E1**	
Dateischleuse: Typen* **Hinweis:** Dieser Menüpunkt ist nur dann verfügbar, wenn die Nutzung der Dateischleuse nicht deaktiviert wurde.	Filtereinstellung zur Steuerung der Dateitypen, die über die Schleuse in das interne Netz und vom internen Netz auf TightGate®-Pro Server transferiert werden dürfen. Die Erkennung der Dateitypen in der Filterfunktion der Schleuse geschieht anhand der MIME-Typen. Der Dateitypenfilter kann ausschließlich für den Transfer von TightGate®-Pro Server zum Arbeitsplatz (Klientenrechner) granular eingestellt werden. In umgekehrter Richtung gibt es nur die Einstellung erlaubt/nicht erlaubt. Dieses An- bzw. Abstellen des Filters vom Arbeitsplatz zum TightGate®-Pro Server geschieht über den Dateityp application/x-empty. Eine Liste der auswählbaren MIME-Typen enthält der Anhang zu diesem Administrationshandbuch, der in einem gesonderten Dokument verfügbar ist. **Hinweis:** Sobald wenigstens ein Dateityp ausgewählt wurde, ist der Filter sofort aktiv. Alle nicht ausgewählten Dateitypen werden blockiert und können mittels der Dateischleuse nicht mehr in das interne Netz transferiert werden. Eine Mehrfachauswahl ist möglich. Die Prüfung der Dateien erfolgt anhand ihres MIME-Typs, unabhängig von der gewählten Dateierweiterung.	**nc**	**E1**	

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Benutzerprofil: Vorgabe* **Hinweis:** Dieser Menüpunkt ist nur dann verfügbar, wenn außer dem Profil „Standard“ noch ein Profil „Custom“ installiert ist.	TightGate®-Pro Server bietet die Möglichkeit, zwischen mehreren Benutzerprofilen auszuwählen. Jedes Benutzerprofil stellt einen definierten Katalog an Leistungsmerkmalen bereit. So können umfangreiche oder besonders zweckorientierte Benutzerumgebungen realisiert werden. Benutzer finden nur solche Bedienelemente in ihrer Arbeitsumgebung vor, die im Rahmen der täglichen Arbeit tatsächlich benötigt werden. **Hinweis:** Diese Einstellung wirkt sich nur auf Benutzerkonten aus, die manuell oder automatisch neu angelegt werden. Je nach Ausstattung kann TightGate®-Pro Server werkseitig mit unterschiedlichen Profilen ausgestattet sein. Weitere Profile können vom technischen Kundendienst der m-privacy GmbH nachinstalliert werden. Diese erscheinen dann ebenfalls als Auswahlmöglichkeit unter diesem Menüpunkt. **Achtung:** Im Profil „Custom“ sind, sofern installiert, die Optionen für die LXDE-Oberfläche sowie weitere Einstellungen für die Menüleiste fest vordefiniert. Werden Benutzerkonten mit einem solchen Profil neu angelegt bzw. zurückgesetzt, greift das System hierzu ausschließlich auf die im Profil definierten Vorgaben zurück. Hierdurch sind anwendungsspezifische Profile möglich, die sich weitreichend von den Standardprofilen unterscheiden.		**E1**	
LXDE-Optionen: Vorgabe*	Legt fest, welche Bedienelemente auf dem Desktop neu angelegter Benutzerkonten verfügbar sind.		**E1**	
Drucken in Spool: Vorgabe	Legt fest, ob neu angelegte Benutzerkonten in das Spool-Verzeichnis oder direkt auf einen Drucker ausdrucken sollen. **Hinweis:** Im ersten Fall ist zur weiteren Verarbeitung die entsprechende Klientensoftware zur Spool-Verarbeitung erforderlich und auf den Klientenrechnern zu installieren, da andernfalls keine Druckausgabe erfolgen kann.		**E1**	
Drucken in Spool: Intervall	Einstellung des Polling-Intervalls des Druckspoolers in Sekunden. Empfohlener Wert: 30 – 60.		**E6**	**F6**
Direkten PDF-Druck erlauben*	Wird diese Option auf „Ja“ gesetzt, werden PDF-Dateien ohne weitere Umwandlung in das Spool-Verzeichnis des Klienten geschrieben und dort zum Ausdruck übernommen. Bei Abwahl dieser Option wird eine PDF-Datei zunächst serverseitig von einem PDF-Anzeigeprogramm geöffnet und als neu generierte PDF-Datei ins Spool-Verzeichnis des Klienten übertragen. Durch diesen Zwischenschritt wird möglicher Schadcode recht zuverlässig eliminiert. Allerdings werden verschlüsselte PDF-Dateien oder solche mit Einschränkungen und Sonderfunktionen mitunter nicht korrekt ausgegeben.		**E1**	
Zwischenablage*	Einstellung der zugelassenen Übertragungswege bei Verwendung der Zwischenablage.		**E1**	
Zwangstrennung für Inaktive*	Zeit in Sekunden, bis inaktive VNC-Verbindungen (Verbindungen der Klientenrechner mit TightGate®-Pro) getrennt werden (voreingestellt sind 36000 s = 10 Stunden).		**E6**	**F6**

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Maximale Sitzungsdauer*	Zeit in Sekunden, bis VNC-Verbindungen (Verbindungen der Klientenrechner mit TightGate®-Pro) in jedem Fall getrennt werden (voreingestellt sind 86400 s = 24 Stunden). Eine sofortige Neuanmeldung ist möglich, der Benutzer erhält dann einen entsprechenden Hinweis über den Grund der Trennung.		**E6**	**F6**
Bildverzögerung*	Verzögerung der Bildaktualisierung in Millisekunden. Der Standardwert von 40 Millisekunden sollte nur in begründeten Fällen geändert werden. Geringere Werte erhöhen den Bandbreitenbedarf pro angemeldetem Klientenrechner.		**E6**	**F6**
Magische URLs*	Ist nur dann zu aktivieren, wenn die teilautomatische Browserweiche auf den Klientenrechnern genutzt werden soll. **Achtung:** Es ist zusätzlich das MSI-Paket für MagicURL auf den Klientenrechnern zu installieren und die Positivliste (WhiteList) über den integrierten Editor klientenseitig mit den als intern zu behandelnden URLs zu füllen. **Warnung:** Für TightGate®-Pro (CC) Version 1.4 Server muss diese Option ausgeschaltet bleiben, da die CC-Konformität andernfalls verloren geht.		**E1**	
Transfer: Lebensdauer*	Zeit in Tagen, die Dateien von Benutzern im Ordner für Transfer-Dateien /transfer (Dateischleuse) aufbewahrt werden sollen. Nach Ablauf dieser Zeit werden die Dateien automatisch gelöscht. Der Eintrag von Null Tagen führt zu einer unbegrenzten Aufbewahrungszeit, d.h. es erfolgt keine automatische Löschung. **Warnung:** Bei intensiver Systemnutzung durch zahlreiche Benutzer kann es zu Betriebsstörungen infolge Überschreitung des verfügbaren Festplattenplatzes kommen, wenn die zeitgesteuerte Löschung von Dateien deaktiviert wird.		**E6**	**F6**

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Audio-Unterstützung*	Globale Aktivierung der Audio-Unterstützung für die VNC-Benutzer von TightGate®-Pro Server. Ob Audio für den jeweiligen Benutzer tatsächlich verfügbar ist, wird durch ***maint*** individuell pro Benutzer eingestellt. In TightGate®-Pro (CC) Version 1.4 Server ist die Audiounterstützung standardmäßig deaktiviert. **Warnung:** Die Audio-Übertragung zwischen TightGate®-Pro Server und den Klientenrechnern erfolgt stets unverschlüsselt. Daher eignet sich das System explizit nicht zur Übertragung vertraulicher Audio-Inhalte. **Achtung:** Falls die Audio-Wiedergabe über TightGate®-Pro generell nicht gewünscht oder nicht erforderlich ist, muss sie an dieser Stelle global deaktiviert werden. Wird lediglich der Netzwerkport 4713 zur Übertragung der Tonsignale per Paketfilter blockiert, kommt es zu Störungen bei der Videowiedergabe mit TightGate®-Pro. Dies kann durch Abschalten der Audio-Unterstützung mittels dieser Einstelloption vermieden werden. Nach korrekter Deaktivierung der Audio-Unterstützung ist der Netzwerkport 4713 für die korrekte Funktion von TightGate®-Pro Server nicht mehr erforderlich. **Hinweis:** Ist die Audiounterstützung an dieser Stelle deaktiviert, bleiben die benutzerindividuellen Einstellungen als Administrator ***maint*** ohne Wirkung. Die Klienten können in diesem Fall keine Tonsignale wiedergeben. Zu beachten ist weiterhin, dass auch nach Aktivierung der Audiowiedergabe mittels dieser Einstelloption noch zusätzlich benutzerindividuelle Einstellungen als Administrator ***maint*** vorzunehmen sind. Es darf nicht automatisch davon ausgegangen werden, dass sämtliche Benutzer Tonsignale wiedergeben können, wenn die globale Audiounterstützung als Administrator ***config*** aktiviert wurde.		**E1**	
Pulseaudio Extra-Ports	Auswahl zusätzlicher Port-Bereiche, die außer des Ports 4713 verwendet werden dürfen. Der letztlich verwendete Port wird durch den VNC-Klienten bestimmt. Ohne Auswahl wird ausschließlich der Standard-Port 4713 verwendet. **Hinweis:** Diese Einstelloption dient insbesondere zur Durchleitung von Audiosignalen an Klienten eines Terminalservers (z. B. CITRIX).		**E1**	
Benutzer-Shell erlauben*	Erlaubt den Start einer Eingabeaufforderung durch die Benutzer.	**nc**	**E1**	
Zeitserver für Klienten*	In der Regel kann diese Einstellung deaktiviert bleiben. Die Freigabe eines Zeitservers über TightGate®-Pro Server kann erforderlich werden, wenn ausnahmslos der gesamte Netzwerkverkehr zu den Arbeitsplatzrechnern zwangsläufig über TightGate®-Pro Server geführt wird (sogenannter „Enforcing“-Modus).		**E1**	
Nagios-NRPE-Unterstützung*	Wenn der ReCoBS-Server durch den System-Überwachungsdienst Nagios überwacht werden soll, muss diese Einstellung aktiviert sein. Bei Nutzung der automatischen Lastverteilung im Cluster ist NRPE zwingend erforderlich.		**E1**	

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
SNMP-Dienst starten*	Aktiviert oder deaktiviert den SNMP-Dienst zur Überwachung von TightGate®-Pro Server über das Netzwerk. **Hinweis:** Die Nutzung des SNMP-Dienstes beschränkt sich auf Statusabfragen. Es ergibt sich hieraus keine Sicherheitsimplikation für den Betrieb von TightGate®-Pro Server.		**E1**	

4.4.4 Administrationsvorgaben

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Fernadministration*	Aktivierung des SSH-Zugangs zur Wartung aktivieren oder deaktivieren.	**nc**	**E1**	
Wartung und Updates(*)	Hier wird das Zugangsverfahren zum Updateserver eingestellt, um Fernwartungsarbeiten ausführen oder Updates für den TightGate®-Pro Server einspielen zu können. Fernwartung ist üblicherweise nur nach zusätzlicher Freischaltung durch den Administrator ***maint*** möglich. **Hinweise:** Die betreffenden Einstellungen gelten bei Rechnerverbünden (Cluster-Systemen) für alle Knoten (Nodes), mit Ausnahme der Untermenüoption ***config > Einstellungen > Wartung und Updates > Umgeleiteter ferner Port***. Diese Einstellung wird für jeden Knoten individuell vorgenommen, damit mehrere Knoten zur gleichen Zeit ferngewartet werden können. **Warnung:** Diese Einstellungen sollten nur in Absprache mit dem technischen Kundendienst der m-privacy GmbH vorgenommen und unmittelbar anschließend sorgfältig auf korrekte Funktion überprüft werden. Fehlerhafte Einstellungen können zu Betriebsstörungen und Sicherheitsrisiken führen. **Achtung:** Bei TightGate®-Pro (CC) Version 1.4 Server muss der Zugriff zur Fernwartung zum Erhalt der CC-Konformität von einem Rechner außerhalb des Klientennetzes ausgeführt werden. Dessen IPv4-Adresse ist unter ***config > Einstellungen > Wartung und Updates > Nagios / Storage IP*** zu hinterlegen, da andernfalls kein Zugriff auf TightGate®-Pro (CC) Version 1.4 Server von Rechnern außerhalb des Klientennetzwerks möglich ist.		**E1 E3 E5 E6**	**F3 F5 F6**
Neustart (zeitgesteuert)	TightGate®-Pro Server kann bei Bedarf turnusmäßig neu gestartet werden. Nach Auswahl eines Wochentags kann auch die gewünschte Stunde hinterlegt werden. Wird kein Wochentag ausgewählt, erfolgt generell kein automatischer Neustart. **Hinweis**: Ein regelmäßiger Neustart ist aus technischer Sicht nicht erforderlich, kann aber durch lokale Vorschriften gefordert sein. **Achtung**: Bei einem Cluster sollten alle Knoten entweder gleichzeitig (Dienstunterbrechung!) oder im Abstand von mindestens einer Stunde neu gestartet werden, da sonst Störungen bis hin zu einem Datenverlust auftreten können.		**E1 E2**	**F0**

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Cluster-Einstellungen	Konfigurationsparameter im Zusammenhang mit einem Verbundrechnersystem. Diese Einstellung wird werkseitig vorgenommen. **Hinweis:** Bei aktiviertem Verbundrechnersystem erhalten sämtliche Einstelloptionen, die für den gesamten Verbund gelten, zur Kennzeichnung die Markierung (*).		**E1 E2 E4 E5 E6**	**F5 F6 F8**
Statusseite: Passwort*	Wird an dieser Stelle ein Passwort gesetzt, muss es zum Aufruf der Statusseite von TightGate®-Pro Server klientenseitig unter http://localhost eingegeben werden. **Hinweis:** Die Systemstatistiken auf der Statusseite werden im Stundenrhythmus aktualisiert. Kurzfristige Änderungen sind daher unter Umständen nicht sichtbar.		**E2 E4**	

Achtung: Nach Verlassen der jeweiligen Menüs muss der aktuelle Stand der Einstellungen jeweils explizit mit der Menüoption ***Speichern*** gesichert werden. Anschließend bewirkt die Menüoption ***Sanft Anwenden*** die Aktivierung der gespeicherten Einstellungen einschließlich etwaiger Änderungen.

Hinweis:
Nach Änderung von Netzwerkkarten-Treibern muss TightGate®-Pro Server neu gestartet werden. Die notwendigen Einstellungen können im laufenden Betrieb zwar gespeichert, jedoch erst nach einem Neustart übernommen werden.

4.5 Authentisierungsmethoden und Single Sign-on (SSO)

Warnung: Die Konfiguration der Authentifizierung über LDAP oder Kerberos-5 ist nur durch fachkundiges Personal vorzunehmen. Fehlerhafte Einstellungen können zu erheblichen Betriebsstörungen führen. Aufgrund der Komplexität der Anmeldemethoden wird empfohlen, den technischen Kundendienst der m-privacy GmbH zurate zu ziehen.

Die Authentisierungsmethoden werden als Administrator ***config*** unter den Menüpunkt ***Einstellungen > Authentisierungs-Methode*** eingestellt. Es bestehen derzeit vier Möglichkeiten, die Benutzer an TightGate®-Pro Server zu authentifizieren:

- RSBAC: Authentisierung der Benutzer durch die lokale Benutzerverwaltung
- LDAP: Authentisierung der Benutzer durch einen LDAP-Server im Netzwerk
- Kerberos-5: Authentisierung der Benutzer durch einen Active-Directory-Server oder ein anderes Kerberos-System im Netzwerk
- AD: Authentisierung der Benutzer durch einen Active-Directory-Server einschließlich Single Sign-on. Wird letztere Option nicht benötigt, kann auch Kerberos-5 gewählt werden. Dann ist nur die Authentisierung gegen das AD mit Benutzername und Passwort möglich. Die in diesem Menü vorhandenen LDAP-Einstellungen bleiben späteren Erweiterungen vorbehalten.

Hinweis: Die Untermenüs im Hauptmenüpunkt ***Authentisierung*** werden je nach gewählter Methode hinsichtlich der verfügbaren Einstelloptionen angepasst.

4.5.1 RSBAC-Authentisierung

Für die RSBAC-Authentisierung sind folgende Einstellungen im Menü vorzunehmen:

config > Einstellungen > Authentisierung	
Menüpunkt	**Beschreibung**
Zurück	Rückkehr zum Hauptmenü.
Authentsierungs-Methode*	RSBAC Die Benutzerverwaltung erfolgt mit dieser Einstellung über das in TightGate®-Pro Server integrierte System. **Hinweis:** Entsprechend dieser Auswahl werden die übrigen Menüpunkte angepasst. Wird das Untermenü später erneut aufgerufen, werden nur die Menüpunkte angezeigt, die zur jeweiligen Auswahl in diesem Feld passen.
Benutzer-Zertifikate automatisch*	Mit Aktivierung dieser Einstelloption wird für jeden neu angelegten Benutzer automatisch ein SSL-Zertifikat zum Single Sign-on erzeugt. Zur alternativen Verwendung des in TightGate®-Pro Server integrierten SSO-Authentisierungssystems.
Auto-Wiederverbinden im Zertifikat	Bei Auswahl dieser Einstelloption werden die auf TightGate®-Pro Server generierten Zertifikate mit einer Information versehen, die den TightGate®-Viewer zu einer automatischen Neuanmeldung veranlasst, sollte die Verbindung abbrechen.
Benutzerverz. automatisch*	Bei Aktivierung dieser Einstelloption wird automatisch ein Benutzerkonto angelegt, sobald eine Anmeldung an TightGate®-Pro Server mit einem vorab erstellten Massenzertifikat erfolgt. Wird diese Einstelloption deaktiviert, kann über manuelles Anlegen der jeweiligen Benutzerkonten gesteuert werden, zu welchem Zeitpunkt ein (ggf. bereits vorab auf die Arbeitsplatzrechner verteiltes) Zertifikat die Anmeldung an TightGate®-Pro Server tatsächlich ermöglichen soll.
Lesezeichen-Archiv	Aktiviert die automatische Archivierung von Lesezeichen (Dateien places.sqlite und bookmarkbackups) in ***/home/user/.bookmarks/<Benutzername>/***. Wird eine Benutzerkennung gelöscht und später unter gleichem Bezeichner automatisch neu angelegt, werden die archivierten Lesezeichen wieder einkopiert. **Hinweis:** Sollten die Archivdaten unbrauchbar werden, kann das Benutzerkonto durch den Administrator ***maint*** zurückgesetzt werden. Anschließend kann der betreffende Benutzer seine Lesezeichen manuell aus dem Backup wieder herstellen. Sollte die interne Lesezeichen-Datenbank unbrauchbar sein, wird bei der Anmeldung des Benutzers automatisch zuerst auf das Lesezeichen-Archiv und schließlich auf die Profil-Einstellungen zurückgegriffen.

Windows-Cursor in Klienten-Konfig.	Mit Aktivierung dieser Einstelloption wird die Darstellung des Mauszeigers auf Klientenrechnern verbessert, wenn diese an einen CITRIX-Terminalserver angeschlossen sind, der in VNC-Verbindung mit TightGate®-Pro Server steht. Im Fall einer solchen „Remote-Kaskade“ kann es andernfalls zu Verzögerungen bei der Darstellung des Mauszeigers bzw. zu Doppeldarstellungen kommen. Bei direkter Verbindung der Klientenrechner zu TightGate®-Pro Server (Installation des Viewer-Programms auf dem Klientenrechner) ist diese Einstelloption zu deaktivieren. **Achtung:** Die SSO-Zertifikate für alle Klienten, die nach Setzen dieser Option den Windows-Cursor nutzen sollen, müssen neu erzeugt und verteilt werden. Erst damit werden die Viewer-Programme auf den Klientenrechnern entsprechend umgestellt. Alle nach Setzen der Option automatisch neu erzeugten Zertifikate enthalten diese Option bereits. **Hinweis:** Bei allen anderen Authentisierungsarten, die nicht auf den seitens TightGate®-Pro Server generierten Zertifikaten zum Single Sign-on (SSO) beruhen, ist diese Einstelloption ohne Bedeutung, weil die Einstellung im Zertifikat gespeichert und den Viewer auf dem Klienten nicht erreichen würde. Kommen andere authentisierungsarten als „RSBAC“ zum Einsatz und soll die Windows-Cursor-Option verwendet werden, müssen die Viewer-Programme auf den Klientenrechnern manuell per Programm-Menü oder per Konfigurationsdatei umgestellt werden. Gegebenenfalls kann der technische Kundendienst ein MSI-Paket bereitstellen, welches den entsprechend konfigurierten Viewer bereits enthält.
Lokales Passwort*	Diese Einstelloption legt fest, ob ein Anmeldung mit Benutzername und Passwort zulässig sein soll. Sofern die zertifikatsbasierte Anmeldung gewählt wurde, kann auf diese Option verzichtet werden. Parallele Verwendung von zertifikatsbasierter und passwortbasierter Anmeldung ist jedoch grundsätzlich möglich. **Achtung:** Steht diese Option auf „Ja“, d. h. ist ein lokales Passwort grundsätzlich zulässig, muss es zwingend gesetzt werden und darf nicht abgelaufen sein. Andernfalls ist die Anmeldung eines VNC-Benutzers an TightGate®-Pro Server – auch per Single Sign-on – nicht möglich!
Mehrere Transfer-Benutzer*	Wird diese Option aktiviert, kann ***maint*** für bis zu 99 unabhängige ***transfer***-Benutzer Kennworte festlegen. **Achtung:** Die ***transfer***-Benutzer werden erst dann im Menü des Administrators ***maint*** angezeigt, nachdem dessen Konsolensitzung neu gestartet wurde. Für TightGate®-Pro (CC) Version 1.4 Server gelten besondere Regelungen für den Dateitransfer.
Erlaubte Benutzer-IDs	Auswahl zwischen mehreren Bereichen, in denen TightGate®-Pro Server UIDs für angemeldete Benutzer zuweist. Namen von Benutzerkonten, die nur aus Ziffern bestehen, können sich nicht im ausgewählten Wertebereich befinden.
Schwache Verschlüsselung zulassen*	Wird der Vorgabewert „Ja“ beibehalten, lässt TightGate®-Pro Server auch eine Verbindung von Klienten mit schwacher Verschlüsselung zu. Dies ist speziell für ältere Klienten-Konfigurationen unter Windows® XP erforderlich, da andernfalls keine Verbindung mit Klientenrechnern möglich ist. Es wird auch in diesem Fall vorzugsweise die starke Verschlüsselung verwendet, sofern durch den jeweiligen TightGate®-Pro Client auf dem Klientenbetriebssystem unterstützt. Der Vorgabewert kann daher im Regelfall beibehalten werden. Auf Wunsch kann durch Wechsel auf die Einstellung „Nein“ die starke Verschlüsselung erzwungen werden. **Achtung:** Bei erzwungener starker Verschlüsselung wird eine Verbindung zu älteren Klienten-Konfigurationen unter Windows® XP von TightGate®-Pro Server abgewiesen. Bei ungeklärten Verbindungsproblemen sollte diese Einstellung geprüft und der Vorgabewert „Ja“ beibehalten werden.

Achtung: Nach Verlassen der jeweiligen Menüs muss der aktuelle Stand der Einstellungen explizit mit der Menüoption ***Speichern*** gesichert werden. Anschließend bewirkt die Menüoption ***Sanft Anwenden*** die Aktivierung der gespeicherten Einstellungen einschließlich etwaiger Änderungen.

4.5.2 LDAP-Authentisierung

config > Einstellungen > Authentisierung	
Menüpunkt	**Beschreibung**
Zurück	Rückkehr zum Hauptmenü.
Authentisierungs-Methode*	LDAP: Die Benutzer werden auf dem TightGate®-Pro Server angelegt, die Passwortauthentisierung erfolgt aber gegen einen LDAP-Server. **Hinweis:** Entsprechend dieser Auswahl werden die übrigen Menüpunkte angepasst. Wird das Untermenü später erneut aufgerufen, werden nur die Menüpunkte angezeigt, die zur jeweiligen Auswahl in diesem Feld passen.
Benutzer-Zertifikate automatisch*	Mit Aktivierung dieser Einstelloption wird für jeden neu angelegten Benutzer automatisch ein SSL-Zertifikat zum Single Sign-on erzeugt. Zur alternativen Verwendung des in TightGate®-Pro Server integrierten SSO-Authentisierungssystems.
Auto-Wiederverbinden im Zertifikat	Bei Auswahl dieser Einstelloption werden die auf TightGate®-Pro Server generierten Zertifikate mit einer Information versehen, die den TightGate®-Viewer zu einer automatischen Neuanmeldung veranlasst, sollte die Verbindung abbrechen.
Benutzerverz. automatisch*	Bei Aktivierung dieser Einstelloption wird automatisch ein Benutzerkonto angelegt, sobald eine Anmeldung an TightGate®-Pro Server mit einer im LDAP hinterlegten Benutzerkennung erfolgt. Wird diese Einstelloption deaktiviert, kann über manuelles Anlegen der jeweiligen Benutzerkonten gesteuert werden, zu welchem Zeitpunkt eine (ggf. bereits vorab auf LDAP angelegte) Benutzerkennung die Anmeldung an TightGate®-Pro Server tatsächlich ermöglichen soll.
Lesezeichen-Archiv	Aktiviert die automatische Archivierung von Lesezeichen (Dateien places.sqlite und bookmarkbackups) in ***/home/user/.bookmarks/<Benutzername>/***. Wird eine Benutzerkennung gelöscht und später unter gleichem Bezeichner automatisch neu angelegt, werden die archivierten Lesezeichen wieder einkopiert. **Hinweis:** Sollten die Archivdaten unbrauchbar werden, kann das Benutzerkonto durch den Administrator ***maint*** zurückgesetzt werden. Anschließend kann der betreffende Benutzer seine Lesezeichen manuell aus dem Backup wieder herstellen. Sollte die interne Lesezeichen-Datenbank unbrauchbar sein, wird bei der Anmeldung des Benutzers automatisch zuerst auf das Lesezeichen-Archiv und schließlich auf die Profil-Einstellungen zurückgegriffen.
Windows-Cursor in Klienten-Konfig.	Die Einstelloption ist bei diesem Authentisierungsverfahren ohne Bedeutung und kann abgeschaltet werden. **Hinweis:** Bei allen Authentisierungsarten, die nicht auf den seitens TightGate®-Pro Server generierten Zertifikaten zum Single Sign-on (SSO) beruhen, ist diese Einstelloption ohne Bedeutung, weil die Einstellung im Zertifikat gespeichert und den Viewer auf dem Klienten nicht erreichen würde. Kommen andere authentisierungsarten als „RSBAC“ zum Einsatz und soll die Windows-Cursor-Option verwendet werden, müssen die Viewer-Programme auf den Klientenrechnern manuell per Programm-Menü oder per Konfigurationsdatei umgestellt werden. Gegebenenfalls kann der technische Kundendienst ein MSI-Paket bereitstellen, welches den entsprechend konfigurierten Viewer enthält.

config > Einstellungen > Authentisierung	
Menüpunkt	**Beschreibung**
Lokales Passwort*	Diese Einstelloption legt fest, ob eine Anmeldung mit Benutzername und Passwort zulässig sein soll. Sofern die zertifikatsbasierte Anmeldung gewählt wurde, kann auf diese Option verzichtet werden. Parallele Verwendung von zertifikatsbasierter und passwortbasierter Anmeldung ist jedoch grundsätzlich möglich. **Achtung:** Steht diese Option auf „Ja“, d. h. ist ein lokales Passwort grundsätzlich zulässig, muss es zwingend gesetzt werden und darf nicht abgelaufen sein. Andernfalls ist die Anmeldung eines VNC-Benutzers an TightGate®-Pro Server – auch per Single Sign-on – nicht möglich!
Mehrere Transfer-Benutzer*	Wird diese Option aktiviert, kann ***maint*** für bis zu 99 unabhängige ***transfer***-Benutzer Kennworte festlegen. **Achtung:** Die ***transfer***-Benutzer werden erst dann im Menü des Administrators ***maint*** angezeigt, nachdem dessen Konsolensitzung neu gestartet wurde. Für TightGate®-Pro (CC) Version 1.4 Server gelten besondere Regelungen für den Dateitransfer.
Erlaubte Benutzer-IDs	Auswahl zwischen mehreren Bereichen, in denen TightGate®-Pro Server UIDs für angemeldete Benutzer zuweist. Namen von Benutzerkonten, die nur aus Ziffern bestehen, können sich nicht im ausgewählten Wertebereich befinden.
LDAP Authentisierungs-Bind-DN*	Benutzername und Passwort zum Zugriff auf die LDAP-Passwortdatenbank.
LDAP Base*	Name der LDAP default base DN (z. B. dc=example, dc=com).
LDAP Server-Netzwerke*	Falls die LDAP-Server mit DNS-Namen angegeben werden, z.B. wegen einer Lastverteilung, sind hier die möglichen IP-Netze einzutragen.
LDAP Server 1*	DNS oder IPv4
LDAP Protokoll 1*	Auswahl zwischen dem ungesicherten LDAP (Port 389) oder einer gesicherten LDAPS-Verbindung (Port 636, LDAP durch SSL getunnelt).
LDAP Server 2*	DNS oder IPv4
LDAP Protokoll 2*	Auswahl zwischen dem ungesicherten LDAP (Port 389) oder einer gesicherten LDAPS-Verbindung (Port 636, LDAP durch SSL getunnelt).

Achtung: Nach Verlassen der jeweiligen Menüs muss der aktuelle Stand der Einstellungen explizit mit der Menüoption ***Speichern*** gesichert werden. Anschließend bewirkt die Menüoption ***Sanft Anwenden*** die Aktivierung der gespeicherten Einstellungen einschließlich etwaiger Änderungen.

4.5.3 Kerberos-5-Authentisierung

Für die Kerberos-5-Authentisierung sind folgende Einstellungen im Menü vorzunehmen:

config > Einstellungen > Authentisierung		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Zurück	Rückkehr zum Hauptmenü.		**E0**	
Authentisierungs-Methode*	Kerberos-5: Die Benutzer werden auf dem TightGate®-Pro Server angelegt, die Authentisierung erfolgt gegen einen Active Directory Server (Win2003).		**E1**	
Benutzer-Zertifikate automatisch*	Mit Aktivierung dieser Einstelloption wird für jeden neu angelegten Benutzer automatisch ein SSL-Zertifikat zum Single Sign-on erzeugt. Zur alternativen Verwendung des in TightGate®-Pro Server integrierten SSO-Authentisierungssystems.		**E1**	

config > Einstellungen > Authentisierung		**Hinweise**		
Auto-Wiederverbin-den im Zertifikat	Bei Auswahl dieser Einstelloption werden die auf TightGate®-Pro Server generierten Zertifikate mit einer Information versehen, die den TightGate®-Viewer zu einer automatischen Neuanmeldung veranlasst, sollte die Verbindung abbrechen.		**E1**	
Benutzerverz. automatisch*	Bei Aktivierung dieser Einstelloption wird automatisch ein Benutzerkonto angelegt, sobald eine Anmeldung an TightGate®-Pro Server über Kerberos bzw. mit einer im Active Directory hinterlegten Benutzerkennung erfolgt. Wird diese Einstelloption deaktiviert, kann über manuelles Anlegen der jeweiligen Benutzerkonten gesteuert werden, zu welchem Zeitpunkt ein Kerberos-Konto oder eine (ggf. bereits vorab im Active Directory hinterlegte) Benutzerkennung die Anmeldung an TightGate®-Pro Server tatsächlich ermöglichen soll.		E1	
Lesezeichen-Archiv	Aktiviert die automatische Archivierung von Lesezeichen (Dateien places.sqlite und bookmarkbackups) in ***/home/user/.bookmarks/<Benutzername>/***. Wird eine Benutzerkennung gelöscht und später unter gleichem Bezeichner automatisch neu angelegt, werden die archivierten Lesezeichen wieder einkopiert. **Hinweis:** Sollten die Archivdaten unbrauchbar werden, kann das Benutzerkonto durch den Administrator ***maint*** zurückgesetzt werden. Anschließend kann der betreffende Benutzer seine Lesezeichen manuell aus dem Backup wieder herstellen. Sollte die interne Lesezeichen-Datenbank unbrauchbar sein, wird bei der Anmeldung des Benutzers automatisch zuerst auf das Lesezeichen-Archiv und schließlich auf die Profil-Einstellungen zurückgegriffen.		**E1**	
Windows-Cursor in Klienten-Konfig.	Die Einstelloption ist bei diesem Authentisierungsverfahren ohne Bedeutung und kann abgeschaltet werden. **Hinweis:** Bei allen Authentisierungsarten, die nicht auf den seitens TightGate®-Pro Server generierten Zertifikaten zum Single Sign-on (SSO) beruhen, ist diese Einstelloption ohne Bedeutung, weil die Einstellung im Zertifikat gespeichert und den Viewer auf dem Klienten nicht erreichen würde. Kommen andere authentisierungsarten als „RSBAC“ zum Einsatz und soll die Windows-Cursor-Option verwendet werden, müssen die Viewer-Programme auf den Klientenrechnern manuell per Programm-Menü oder per Konfigurationsdatei umgestellt werden. Gegebenenfalls kann der technische Kundendienst ein MSI-Paket bereitstellen, welches den entsprechend konfigurierten Viewer enthält.		**E1**	
Lokales Passwort*	Diese Einstelloption legt fest, ob eine Anmeldung mit lokalem RSBAC-Passwort zulässig sein soll. Sofern die zertifikatsbasierte Anmeldung gewählt wurde, kann auf diese Option verzichtet werden. Parallele Verwendung von zertifikatsbasierter und passwortbasierter Anmeldung ist jedoch grundsätzlich möglich. **Achtung:** Steht diese Option auf „Ja“, d. h. ist ein lokales Passwort grundsätzlich zulässig, muss es zwingend gesetzt werden und darf nicht abgelaufen sein. Andernfalls ist die Anmeldung eines VNC-Benutzers an TightGate®-Pro Server – auch per Single Sign-on – nicht möglich!		**E1**	

config > Einstellungen > Authentisierung		Hinweise		
Mehrere Transfer-Benutzer*	Wird diese Option aktiviert, kann ***maint*** für bis zu 99 unabhängige ***transfer***-Benutzer Kennworte festlegen. **Achtung:** Die ***transfer***-Benutzer werden erst dann im Menü des Administrators ***maint*** angezeigt, nachdem dessen Konsolensitzung neu gestartet wurde. Für TightGate®-Pro (CC) Version 1.4 Server gelten besondere Regelungen für den Dateitransfer.		**E1**	
Erlaubte Benutzer-IDs	Auswahl zwischen mehreren Bereichen, in denen TightGate®-Pro Server UIDs für angemeldete Benutzer zuweist. Namen von Benutzerkonten, die nur aus Ziffern bestehen, können sich nicht im ausgewählten Wertebereich befinden.		**E1**	
Kerberos Realm*	Name des Kerberos Realm. Das Kerberos-Realm kann über den Befehl ksetup.exe auf der Kommandozeile angezeigt werden. Das Realm bei Windows Active Directory Servern ist immer komplett in Großbuchstaben zu schreiben.		**E4**	
Kerberos KDC 1*	IPv4-Adresse des ersten Kerberos-Servers (AD-Server).		**E5**	**F5**
Kerberos KDC 2*	IPv4-Adresse des zweiten Kerberos-Servers (AD-Server).		**E5**	**F5**
Kerberos Admin Server*	IPv4-Adresse des Kerberos-Admin-Servers (AD-Server).		**E5**	**F5**
Importiere Kerberos Host Keytab	Eine Keytab-Datei kann direkt importiert werden. Sie muss dazu im Transfer-Verzeichnis des Administrators ***config*** liegen.		**E7**	**F8**

4.5.4 Single Sign-on (SSO) mit TightGate®-Pro

TightGate®-Pro unterstützt die zertifikatsbasierte Anmeldung ohne Eingabe von Benutzername und Passwort für die Klienten-Betriebssysteme Windows und Linux.

Folgende Voraussetzungen sind zur Nutzung der zertifikatsbasierten Anmeldung zu erfüllen:

1. TightGate®-Pro Server und TightGate®-Pro Client müssen sich auf dem aktuellen Softwarestand befinden.
2. Die Nutzung des seitens der m-privacy GmbH bereitgestellten Viewer- und Schleusenprogramms für SSO ist obligatorisch.
3. Ein auflösbarer DNS-Name, unter dem TightGate®-Pro Server aus dem internen Netz angesprochen werden kann, muss vorhanden sein.

Vorbereitungen zur Zertifikatsnutzung

1. Anmeldung als ***config***
2. Eintragung des auflösbaren DNS-Namens für das betreffende System unter ***Einstellungen > SSL-Name im Zertifikat***
3. ***Speichern*** und ***Sanft Anwenden*** durchführen.

Hinweis: Der unter SSL-Name im Zertifikat eingetragene Hostname wird im jeweiligen Zertifikat als Common Name (CN) hinterlegt. Wird der Hostname in der SSL CN geändert, so sind alle Klientenzertifikate neu zu generieren und an die Klienten zu verteilen (oder zumindest auf allen Klienten die Konfigurationsdateien anzupassen). Vor der Erstellung der Klientenzertifikate und deren Verteilung empfiehlt es sich unbedingt, sorgfältig auf Eintragung des richtigen Hostnamens zu achten.

Zertifikate für bestehende Benutzer erzeugen

1. Anmeldung als ***maint***.
2. Unter ***Benutzerverwaltung > Erzeuge SSL-Schlüssel*** für einzelne Gruppen oder alle Benutzer (Gruppe Everyone) SSL-Zertifikate erzeugen.
3. Über Menüpunkt ***Export. SSL-Schlüssel*** die erzeugten Klientenzertifikate in das Transferverzeichnis von ***config*** kopieren.

Zertifikate auf Klienten verteilen

1. Aufruf der Dateischleuse.
2. Anmeldung als ***config***, Wechsel in das Verzeichnis „certs“. Dort befindet sich jeweils ein Ordner mit dem Namen eines jeden angelegten Benutzers mit einer Reihe von Zertifikaten und Konfigurationsdateien. Diese Dateien (nicht der Ordner an sich) sind nach ***%APPDATA %/vnc /*** zu kopieren.

Zertifikate widerrufen

Der Administrator ***maint*** kann unter dem Menüpunkt ***Benutzerverwaltung > Rückruf Zertifikat*** die Zertifikate einzelner Benutzer widerrufen. Nach einem Widerruf ist eine Anmeldung mit den dann ungültigen Zertifikaten weder über Viewer noch über die Schleuse möglich.

Hinweis: Widerrufene Zertifikate können nicht entsperrt oder reaktiviert werden. Nötigenfalls sind neue Zertifikate zu erzeugen und wie oben angegeben abzurufen und zu verteilen. In Clustersystemen wird die Sperre nach einer Wartezeit bis zu 10 Minuten für die Anmeldung des Viewers und die Nutzung der Dateischleuse wirksam.

Achtung: Bereits aufgebaute Verbindungen bleiben im Fall einer Zertifikatssperre bis zur manuellen oder automatischen Abmeldung vom System bestehen. Dies betrifft den Viewer und die Nutzung der Dateischleuse gleichermaßen.

Zertifikate auf Vorrat erzeugen

Alternativ zur Zertifikatserzeugung für bereits vorhandene Benutzerkennungen können Benutzerzertifikate auch in beliebigen Kontingenten im Voraus erzeugt werden. Benutzer können sich damit auch ohne Benutzeraccount an TightGate®-Pro Server anmelden. Dieser wird im Zuge des ersten Anmeldevorgangs automatisch generiert, was den Administrationsaufwand vermindert.

Vorbereitende Maßnahmen:

1. Anmeldung als Administrator ***config*** .
2. Unter ***Einstellungen > Authentisierungsmethode*** zusätzlich den Menüpunkt ***Benutzerverz. automatisch*** auf „ja“ setzen, falls sich die Benutzer mit den neuen Zertifikaten sofort anmelden sollen.
3. ***Speichern*** und ***Sanft Anwenden.***

Die Benutzerzertifikate können als ***maint*** unter dem Menüpunkt

Benutzerveraltung > Massen-SSL-Schlüssel

erzeugt werden. Es startet ein Assistent, der ein Präfix und die Anzahl zu erzeugender Zertifikate abfragt. Der Präfix bildet den konstanten Teil des späteren Benutzernamens, ergänzt um eine laufende Nummer. Diese beginnt bei einem wählbaren Wert und endet bei der Anzahl der zu erzeugenden Zertifikate. Die erzeugten Zertifikate werden automatisch in das Transfer-Verzeichnis von ***config*** kopiert und können dort abgeholt und verteilt werden.

Hinweise:

- Die automatisch generierten Benutzernamen legen bei der ersten Anmeldung mit dem erzeugten Zertifikat eine gleichlautende Benutzerkennung (Benutzerkonto, Account) auf TightGate®-Pro Server an. Diese kann nachträglich nicht verändert werden.
- Es wird keine Benutzerkennung (Account) auf TightGate®-Pro Server erzeugt, solange ein Zertifikat nur generiert, jedoch noch nicht zur Anmeldung an TightGate®-Pro Server verwendet wurde. Die Benutzerverwaltung von TightGate®-Pro Server enthält damit stets nur solche Kennungen, die tatsächlich bereits zur Anmeldung verwendet wurden - unabhängig von der Zahl der im Voraus erzeugten Zertifikate.

4.6 Proxy-Filter (Inhaltsfilter)

Neben der sicheren Darstellung von Inhalten aus dem Internet bietet TightGate®-Pro auch die Möglichkeit zur inhaltlichen Kontrolle und Beschränkung der Internetnutzung. Der Inhaltsfilter von TightGate®-Pro Server arbeitet als Zwangsproxy anhand definierbarer Kriterien. Folgende Kategorien werden dabei berücksichtigt:

- White- und Blacklisten für URLs und Domains (Webseitenfilterung)
- Filtern von Dateiendungen (Dateifilterung)
- Filtern nach Schlagworten und aufgrund von Heuristiken (Inhaltsfilter)
- Filtern abgerufener Dateien (Downloads) anhand ihrer MIME-Typen

Hinweis: Eine vollständige Übersicht der filterbaren MIME-Typen ist dem Anhang zu diesem Administrationshandbuch zu entnehmen, der gesondert verfügbar ist.

4.6.1 Allgemeines zum URL-Filter

Die Funktionsweise des URL-Filters ist ähnlich der eines Spamfilters. Es werden für bestimmte unerwünschte Schlagworte oder Phrasen aus verschiedenen Kategorien Punkte vergeben. Ist die Summe der Punkte höher als ein festgelegter Schwellwert, wird die Seite blockiert. Die zu verwendenden Heuristiken werden nicht manuell gepflegt, sondern auf Wunsch von einem externen Service im Abonnement bezogen (es entstehen ggf. weitere Kosten). Dem Administrator wählt die gewünschten Kategorien und pflegt erforderlichenfalls White- und Blacklisten.

Hinweis: Wird eine reguläre Internetseite vom URL-Filter beanstandet, wird statt des jeweiligen Inhalts eine spezifische Informationsseite eingeblendet, die auf den Grund der Sperre hinweist. Diese Einblendung unterbleibt aus technischen Gründen, falls eine verschlüsselte Seite aufgerufen wird (https://...). Stattdessen erscheint ein unspezifischer Hinweis auf ein vermeintliches Problem mit dem Proxy-Server. Die beanstandeten Inhalte werden ungeachtet dessen in jedem Fall zuverlässig blockiert.

Grenzen des Inhaltsfilters: Ein Inhaltsfilter ist nur so treffsicher wie seine Heuristiken. Diese sind immer statisch und können fein justiert werden. Das System kann jedoch nicht einschätzen, weswegen einzelne Seiten aufgerufen werden. Vereinzelt unerwünschte Sperren sind ebenso wie die gelegentliche Anzeige unerwünschter Inhalte auch bei sorgfältiger Konfiguration nicht völlig auszuschließen. Es ist eine Abwägung vorzunehmen, welche Inhalte in jedem Fall global gesperrt werden sollen und inwiefern Einschränkungen im Produktivbetrieb unter Inhaltsaspekten akzeptabel sind. Im Zweifelsfall sollte die Heuristik toleranter eingestellt und zuverlässig zu blockierende Inhalte in die Blacklist aufgenommen werden.

4.6.2 AD-Authentisierung (Active Directory)

Zur Anbindung von TightGate®-Pro Server an ein Active Directory sind einige Einstellarbeiten im Vorfeld am AD-Server erforderlich, die im **Abschnitt 7 Nutzung von TightGate®-Pro mit Active Directory** eingehend beschrieben werden.

Achtung: Die Einstellungen am AD-Server müssen vorgenommen werden, bevor die Konfiguration an TightGate®-Pro Server angepasst und angewendet wird. Insbesondere die keytab-Datei muss vor dem ***Sanft Anwenden*** im Transfer-Verzeichnis des Administrators ***config*** vorliegen.

Für die Authentisierung über ein Active Directory mit Single Sign-on (SSO) sind auf TightGate®-Pro Server folgende Einstellungen im Menü vorzunehmen:

config > Einstellungen > Authentisierung		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Zurück	Rückkehr zum Hauptmenü.		**E0**	
Authentisierungs-Methode*	AD: Die Authentisierung erfolgt gegen einen Active Directory Server (Windows Server 2008R2).		**E1**	
Benutzer-Zertifikate automatisch*	Mit Aktivierung dieser Einstelloption wird für jeden neu angelegten Benutzer automatisch ein SSL-Zertifikat zum Single Sign-on erzeugt. Zur alternativen Verwendung des in TightGate®-Pro Server integrierten SSO-Authentisierungssystems.		**E1**	
Windows-Cursor in Klienten-Konfig.	Die Einstelloption ist bei diesem Authentisierungsverfahren ohne Bedeutung und kann abgeschaltet werden. **Hinweis:** Bei allen Authentisierungsarten, die nicht auf den seitens TightGate®-Pro Server generierten Zertifikaten zum Single Sign-on (SSO) beruhen, ist diese Einstelloption ohne Bedeutung, weil die Einstellung im Zertifikat gespeichert und den Viewer auf dem Klienten nicht erreichen würde. Kommen andere Authentisierungsarten als „RSBAC“ zum Einsatz und soll die Windows-Cursor-Option verwendet werden, müssen die Viewer-Programme auf den Klientenrechnern manuell per Programm-Menü oder per Konfigurationsdatei umgestellt werden. Gegebenenfalls kann der technische Kundendienst ein MSI-Paket bereitstellen, welches den entsprechend konfigurierten Viewer enthält.		**E1**	
Benutzerverz. automatisch*	Bei Aktivierung dieser Einstelloption wird automatisch ein Benutzerkonto angelegt, sobald eine initiale Anmeldung an TightGate®-Pro Server über Kerberos bzw. mit einer im Active Directory hinterlegten Benutzerkennung erfolgt. Wird diese Einstelloption deaktiviert, kann über manuelles Anlegen der jeweiligen Benutzerkonten gesteuert werden, zu welchem Zeitpunkt ein Kerberos-Konto oder eine (ggf. bereits vorab im Active directory hinterlegte) Benutzerkennung die Anmeldung an TightGate®-Pro Server tatsächlich ermöglichen soll.		**E1**	
Benutzernamen in Kleinbuchstaben*	Bei Aktivierung dieser Einstelloption werden alle Benutzernamen zwangsläufig in Kleinbuchstaben gewandelt. Dies vermeidet insbesondere Komplikationen mit Kerberos-Servern, die Groß- und Kleinschreibung im Gegensatz zu TightGate®-Pro Server nicht unterscheiden.		**E1**	

config > Einstellungen > Authentisierung		**Hinweise**		
Lokales Passwort*	Diese Einstelloption legt fest, ob eine Anmeldung mit lokalem RSBAC-Passwort zulässig sein soll. Sofern die zertifikatsbasierte Anmeldung gewählt wurde, kann diese Option auf „Nein“ stehen. Parallele Verwendung von zertifikatsbasierter und passwortbasierter Anmeldung ist jedoch grundsätzlich möglich. **Achtung:** Steht diese Option auf „Ja“, d. h. ist ein lokales Passwort grundsätzlich zulässig, muss es zwingend gesetzt werden und darf nicht abgelaufen sein. Andernfalls ist die Anmeldung eines VNC-Benutzers an TightGate®-Pro Server – auch per Single Sign-on – nicht möglich!		**E1**	
Mehrere Transfer-Benutzer*	Wird diese Option aktiviert, kann ***maint*** für bis zu 99 unabhängige ***transfer***-Benutzer Kennworte festlegen. **Achtung:** Die ***transfer***-Benutzer werden erst dann im Menü des Administrators ***maint*** angezeigt, nachdem dessen Konsolensitzung neu gestartet wurde. Für TightGate®-Pro (CC) Version 1.4 Server gelten besondere Regelungen für den Dateitransfer.		**E1**	
Erlaubte Benutzer-IDs	Auswahl zwischen mehreren Bereichen, in denen TightGate®-Pro Server UIDs für angemeldete Benutzer zuweist. Namen von Benutzerkonten, die nur aus Ziffern bestehen, können sich nicht im ausgewählten Wertebereich befinden.		**E1**	
Kerberos Realm*	Name des Kerberos Realm. Das Kerberos-Realm kann über den Befehl ksetup.exe auf der Kommandozeile angezeigt werden. Das Realm bei Windows Active Directory Servern ist immer komplett in Großbuchstaben zu schreiben.		**E4**	
Kerberos KDC 1*	IPv4-Adresse des ersten Kerberos-Servers (AD-Server).		**E5**	**F5**
Kerberos KDC 2*	IPv4-Adresse des zweiten Kerberos-Servers (AD-Server).		**E5**	**F5**
Kerberos Admin Server*	IPv4-Adresse des Kerberos-Admin-Servers (AD-Server).		**E5**	**F5**
Kerberos Hostname*	DNS-Name des Kerberos-Servers (meist, aber nicht zwingend der Name eines Einzelsystems oder des Clusters). Spezifisch für die Infrastruktur am Einsatzort. **Achtung:** Bei fehlerhafter Angabe dieses Parameters ist keine Anmeldung möglich. Eine dedizierte Fehlermeldung erfolgt nicht.		**E4**	
Kerberos Service	Bezeichnung des AD-Dienstes innerhalb der Infrastruktur am Einsatzort. Kann frei gewählt werden. **Achtung:** Bei fehlerhafter Angabe dieses Parameters ist keine Anmeldung möglich. Eine dedizierte Fehlermeldung erfolgt nicht.		**E4**	
Importiere Kerberos Host Keytab	Eine Keytab-Datei kann direkt importiert werden. Sie muss dazu im Transfer-Verzeichnis des Administrators ***config*** liegen.		**E7**	**F8**

config > Einstellungen > Authentisierung		Hinweise		
Transfer-MIME-Typen-Gruppen	Definiert Anzahl und Inhalt der Gruppen von MIME-Typen, die AD-gesteuert über die Dateischleuse von TightGate®-Pro Server transferiert werden dürfen. Es können maximal 99 Gruppen angelegt und beliebig mit MIME-Typen bestückt werden. Jeder dieser Gruppen können im Active Directory (AD) Benutzer zugewiesen werden. Ist ein Benutzer in keiner Transfergruppe, kann er keine Dateien über die Dateischleuse übertragen. Die Transferberechtigungen der Gruppen sind kumulativ. **Achtung:** Die Gruppe *tgtransfer* ist stets erforderlich – ihr muss ein Benutzer auf dem AD angehören, um überhaupt zur Dateiübertragung berechtigt zu sein. Dies betrifft auch die automatisch generierten PDF-Dateien der Druckausgabe, die durch den Druckspooler von TightGate®-Pro Server zur Arbeitsplatzstation transferiert werden. In diesem Fall muss zusätzlich die Gruppe *TGTransfer-Spool* existieren und der Benutzer auf dem AD dieser angehören.		**E1** **E6**	
LDAP Base*	Name der LDAP default base DN (z.B. dc=example, dc=com).		**E4**	
LDAP Server-Netzwerke*	Falls die LDAP-Server mit DNS-Namen angegeben werden, z.B. wegen einer Lastverteilung, sind hier die möglichen IP-Netze einzutragen.		**E5**	**F5**
LDAP Server 1*	DNS oder IPv4		**E4** **E5**	**F5**
LDAP Server 2*	DNS oder IPv4		**E4** **E5**	**F5**

4.6.3 Konfiguration des URL-Filters

Zur Aktivierung und Konfiguration des URL-Filters ist die Anmeldung als Administrator ***config*** erforderlich.

config > Einstellungen > Proxy-Filter		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Zurück	Rückkehr zum Hauptmenü.		**E0**	
Aktivieren / Deaktivieren	Ein- bzw. Abschalten des URL-Filters.		**E1**	
Abonnierungs-URL	Link zu Aktualisierungen des URL-Filters. **Hinweis:** Die Bestimmungen zu den jeweils gültigen Lizenzen sind z.B. unter URLBlacklist.com abrufbar.		**E4**	
Abonnierungs-Aktualisierungen	Häufigkeit der Aktualisierungen des URL-Filters. **Hinweis:** Die Bestimmungen zu den jeweils gültigen Lizenzen sind z.B. unter URLBlacklist.com abrufbar.		**E1**	

config > Einstellungen > Proxy-Filter		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Erlaube Umgehen des Filters	Angabe der Zeit in Sekunden, für die eine eigentlich gesperrte Seite für den Benutzer dennoch verfügbar ist. Ruft ein Benutzer eine durch den URL-Filter gesperrte Seite auf, so erscheint ein Fenster mit der Meldung, dass die URL blockiert wurde. Wird der in der Meldung gezeigte Link aufgerufen, erfolgt die Anzeige der betreffenden Seite unabhängig von den Sperreinstellungen. Für die angegebene Zeit ist die Seite dann für den Benutzer voll verfügbar. **Achtung:** Ist hier eine Zeit angegeben, können innerhalb des Zeitfensters sämtliche unerwünschten Inhalte aufgerufen werden. Je nach Anwendungsfall kann die Option „Nein“ für "Gefiltertes Web" eine sinnvollere Alternative sein. Eingabe des Werts 0 verhindert die Umgehung des Inhaltsfilters.		**E6**	**F6**
Schwellwert	Der Inhaltsfilter bildet anhand verschiedener Inhaltskriterien eines Webangebots einen Punktewert. Der Schwellwert ist der Punktewert, ab dem eine Seite blockiert wird. Die Tabelle der Schwellwerte für beispielhafte Inhalte kann als Orientierung dienen. In der Praxis müssen geeignete Schwellwerte zumeist anhand exemplarischer Webinhalte empirisch ermittelt werden.		**E6**	**F6**
Zugriff-Verweigert-Text	Text, der den Benutzern auf der Hinweisseite in der zweiten Spalte angezeigt wird. **Hinweis**: Hier sollte ein administrativer Kontakt, z.B. die Telefonnummer des lokalen Helpdesk, angezeigt werden, damit Benutzer irrtümlich gesperrte Seiten melden und bei Bedarf freischalten lassen können.		**E4**	
Kategorien (Phrasen)	Auswahl der zu filternden Kategorien. **Hinweis:** Eine Übersicht über alle Kategorien mit kurzer Beschreibung ist unter http://www.URLBlacklist.com in englischer Sprache zu finden.		**E1**	
Kategorien (Sperrliste)	Auswahl der über den Administrator ***maint*** zu pflegenden White- und Blacklisten. Es können Domains bzw. Adressen einbezogen werden.		**E1**	
Dateiendungs-Blacklist	Auswahl zu verbietender Dateiendungen. Dateiendungen werden nur nach dem Namen, nicht jedoch nach dem Dateityp gefiltert.		**E1**	
MIME-Typen Blacklist	Auswahl zu verbietender Dateitypen. **Achtung:** Diese Auswahl ist nicht mit der Auswahl der Dateitypen für die Schleuse zu verwechseln. Dateitypen, die an dieser Stelle verboten werden, können erst gar nicht aus dem Internet abgerufen werden.		**E1**	

4.6.4 Festlegung des Schwellwertes

Der Schwellwert legt fest, ab welcher Punkteanzahl der URL-Filter Inhalte einer Seite blockiert. Die nachfolgende Übersicht gibt Anhaltspunkte für geeignete Schwellwerte.

Schwellwert	Beschreibung
50	Sehr restriktive Einstellung (geeignet für Kinder).
100	Restriktive Einstellung (geeignet für Jugendliche).
160	Einstellungen für junge Erwachsene.
200	Einstellung für den Normalbetrieb in einer Behörde oder in einem Unternehmen.

4.6.5 Beispielübersicht über Kategorien und Schwellwerte

Die nachfolgende Übersicht stellt ermittelte Schwellwerte des URL-Filters für einzelne bekannte Internetangebote dar.

Hinweis: Die Auswahl der Seiten stellt keine inhaltliche Wertung dar, sondern dient als Orientierungshilfe zum besseren Verständnis zur Festlegung des Schwellwertes.

Hinweis: Die Höhe des Schwellwerts ist nur eine Momentaufnahme zum Zeitpunkt der Erstellung dieser Übersicht. Der Schwellwert einer Seite ändert sich fortwährend mit deren Inhalt.

Internetseite	Schwellwert	Genre
www.bild.de	170	Tageszeitung
www.sueddeutsche.de	190	Tageszeitung
www.web.de	30	Webportal
www.playboy.de	386	Magazin
www.gala.de	10	Magazin
www.brigitte.de	13	Magazin
www.ard.de	10	Funk & Fernsehen
www.sat1.de	10	Funk & Fernsehen
www.prosieben.de	70	Funk & Fernsehen
www.m-privacy.de	5	Sonstige
www.bsi.de	5	Sonstige

Die nachfolgende Übersicht stellt die Auswahl von Kategorien dar, anhand derer die oben angeführten Schwellwerte ermittelt wurden.

Kategorie	Wert
badwords	weighted_german
illegaldrugs	weighted
warezhacking	weighted
nudism	weighted
pornography	weighted, weighted_german
proxies	weighted
violence	weighted

4.6.6 Einstellungen zu White- und Blacklisten (als *maint*)

Vorbereitende Maßnahme: Damit der Webseitenfilter genutzt werden kann, muss dieser zunächst als Administrator ***config*** unter ***config > Einstellungen > Proxy-Filter*** aktiviert werden.

Um einzelne URLs oder Domänen zu den White- oder Blacklisten hinzuzufügen, ist die Anmeldung als Administrator ***maint*** erforderlich.

maint > Webseiten-Filter		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Zurück	Rückkehr zum Hauptmenü.		**E0**	
Anwenden	Alle Einstellungen in diesem Menü sind explizit über diesen Menüpunkt anzuwenden, bevor sie wirksam werden.		**E2**	
Domänen sperren	Eingabe der Domänen, welche vom Inhaltsfilter gesperrt werden sollen. Die Domäne kann dabei auch unter Zuhilfenahme von Wildcards (*) angegeben werden. Beispiel: Die Domäne von EBAY kann für alle Länder mit www.ebay.* komplett verboten werden.		**E1** **E4**	
URLs sperren	Eingabe der URL, welche gesperrt werden soll. **Achtung:** Es werden nur exakt die Seiten gesperrt, die hinterlegt werden. Diese Option ist zur Sperrung kompletter Domänen nicht geeignet.		**E4**	
Domänen freischalten	Diese Einstellung funktioniert analog zur Einstellung für die Sperrung von Domänen.		**E1** **E4**	
URLs freischalten	Diese Einstellung funktioniert analog zur Einstellung für die Sperrung von URLs		**E4**	

4.6.7 Inhaltsfilter für einzelne Benutzer umgehen

TightGate®-Pro Server bietet die Möglichkeit, die Inhaltskontrolle für einzelne Benutzer zu umgehen. Die Umgehung des Inhaltsfilters für einzelne Benutzer wird durch den Administrator ***maint*** unter dem Menüpunkt ***maint > Benutzerverwaltung > Gefiltertes Web*** freigeschaltet.

Achtung: Ist für einen Benutzer der ungefilterte Zugriff auf das Web eingestellt, so erfolgt für diesen Benutzer keinerlei Inhaltskontrolle. Weiterhin muss ein Benutzer sich nach der Umstellung durch ***maint*** erneut an TightGate®-Pro Server anmelden, damit der ungefilterte Webzugriff möglich ist. Der Neustart des Browsers reicht nicht aus.

4.6.8 Filterung anhand von MIME-Typen

MIME ist die Abkürzung für Multipurpose Internet Mail Extensions. Es handelt sich um ein Schema, das TightGate®-Pro Server einen Hinweis auf den verwendeten Datentyp gibt.

Der MIME-Type besteht aus der Angabe eines Medientype und eines Subtype, die durch einen Schrägstrich voneinander getrennt sind. Z.B. text/html oder image/jpeg. TightGate®-Pro Server kann abgerufene Dateien, die in der Dateischleuse abgelegt werden, anhand ihres MIME-Typs zulassen oder blockieren.

Folgende Medientypen gibt es:

Medientype	Beschreibung
application	Dateien, die an ein bestimmtes Anwendungsprogramm gebunden sind
audio	Audio-Dateien
image	Bilder, Grafiken, Fotos
message	Nachrichten
text	Dateien mit ASCII-Text
video	Videodateien

Aus dem Medientype ergibt sich die Art der Datenstruktur, also ob die Daten binär oder nach ASCII abgelegt sind. Der Subtype bezieht sich auf die Dateiformate, die an ein bestimmtes Programm gebunden sind oder mit speziellen Programmen oder Plug-ins ausgeführt werden müssen. Subtypes, die mit einem “x-” beginnen, sind Dateien, die auf einem Server ausgeführt werden.

Hinweis: Eine vollständige Liste der filterbaren MIME-Typen kann dem Anhang zu diesem Administrationshandbuch entnommen werden, der als gesondertes Dokument verfügbar ist.

4.7 Einstellungen zur Nutzung der Dateischleuse

Die Nutzung der Dateischleuse unterliegt einigen zentralen Einstellungen, die systemweit, nutzer- oder gruppenbezogen gelten können. Weiterhin können Dateien über dedizierte ***transfer***-Benutzer zentral übertragen werden, ohne die Schleusenberechtigungen der übrigen Benutzer zu tangieren.

4.7.1 Einstellungen für die individuelle Schleusennutzung

Bei der Verwendung der benutzerindividuellen Dateischleuse können für einzelne Benutzer die Einstellungen für die zum Transfer erlaubten Dateitypen vorgegeben oder geändert werden.

Funktion	Notwendig	Hinweise
Einstellung als ***config*** im Menüpunkt ***Einstellungen > Dateischleuse: Erlauben***	Ja	Diese systemweite Menüoption erlaubt oder verbietet die Nutzung der Dateischleuse für alle Benutzerkonten und hat Vorrang vor gruppen- oder benutzerspzifischen Einstellungen. **Achtung:** Ist die Nutzung der Dateischleuse an dieser Stelle ausgeschaltet, kann kein Benutzer die Schleuse nutzen. Auch die Nutzung des integrierten Druckspoolers ist dann für alle Benutzer deaktiviert! Wird die Schleuse eingeschaltet, gelten die gruppen- und benutzerspezifischen Einstellungen. **Hinweis:** Der dedizierte Schleusen-Benutzer ***transfer*** bleibt von einem Verbot der Schleusennutzung durch diese Einstelloption unbehelligt.

Funktion	Notwendig	Hinweise
Einstellung als ***config*** im Menüpunkt ***Einstellungen > Dateischleuse: Vorgabe***	Nein	Die Einstellung der Dateitransfer-Vorgabe wirkt sich nur auf neu angelegte Benutzerkonten aus. Die Berechtigung zur Schleusennutzung kann gruppenspezifisch oder nutzerindividuell zu einem späteren Zeitpunkt beliebig erteilt oder entzogen werden. **Achtung:** Benutzer, die den integrierten Druckspooler nutzen sollen, benötigen in jedem Fall eine allgemeine Schleusenberechtigung. Es empfiehlt sich, die Vorgabe entsprechend zu setzen.
Einstellung als ***config*** im Menüpunkt ***Einstellungen > Dateischleuse: Typen***	Nein	Die Einstellung der Dateitransfer-Typen wirkt sich ebenfalls nur auf neu angelegte Benutzerkonten aus. Die zugelassenen Dateitypen können gruppenspezifisch oder nutzerindividuell zu einem späteren Zeitpunkt ausgewählt werden. **Hinweis:** Es handelt sich um eine Positivliste. Sobald ein Dateityp ausgewählt wurde, sind automatisch alle nicht ausgewählten Dateitypen verboten. Es ist daher wichtig, sämtliche Dateitypen auszuwählen, die zugelassen werden sollen. Ist keine Einschränkung erforderlich bzw. erwünscht, sollte keine Auswahl getroffen werden.
Aktivierung der Dateischleuse als ***maint*** für einzelne Benutzerkonten oder Gruppen	Ja	Ohne eine allgemeine Schleusenberechtigung kann die Dateischleuse nicht benutzt werden. **Achtung:** Damit der integrierte Druckspooler funktioniert, muss der jeweilige Benutzer eine allgemeine Schleusenberechtigung erhalten.
Auswahl der zulässigen Dateitypen für die Dateischleuse für Benutzer oder Gruppen als ***maint***	Nein	Werden keine Dateitypen ausgewählt, so sind alle Dateitypen zulässig. Daher sollten zur Einschränkung der Schleuse die gewünschten Dateitypen ausgewählt werden. **Hinweis:** Es handelt sich um eine Positivliste. Sobald ein Dateityp ausgewählt wurde, sind automatisch alle nicht ausgewählten Dateitypen verboten. Es ist daher wichtig, sämtliche Dateitypen auszuwählen, die zugelassen werden sollen. Ist keine Einschränkung erforderlich bzw. erwünscht, sollte keine Auswahl getroffen werden.

Hinweis: Für den Austausch von Dateien gilt ein einstellbares Größenlimit von bis zu 4 GB. Größere Dateien werden standardmäßig nicht übertragen. Zu Sonderkonfigurationen erteilt der technische Kundendienst der m-privacy GmbH nähere Auskünfte.

4.7.2 Einstellungen für die zentrale Schleusennutzung

Daten können alternativ auch über den dafür vorgesehenen Benutzer ***transfer*** zentral übertragen werden. Der Benutzer ***transfer*** hat Zugriff auf die Transferverzeichnisse aller Benutzer und kann von dort Dateien in das interne Netz übertragen oder aus dem internen Netz zu TightGate®-Pro Server.

Das Passwort für den Benutzer ***transfer*** wird durch den Administrator ***maint*** in den Benutzereinstellungen unter ***maint > Benutzerverwaltung > Benutzer ändern*** vergeben. Zum Dateitransfer mit dem Benutzer ***transfer*** können die üblichen Programme zur Datenübertragung genutzt werden.

Nach Anmeldung via SFTP als Benutzer ***transfer*** wird eine Auswahl sämtlicher Transfer-Verzeichnisse aller angelegten Benutzerkonten angezeigt. Es können Dateien aus einzelnen Transferverzeichnissen übernommen oder nutzerindividuell hinterlegt werden.

Hinweise:

- Der Benutzer ***transfer*** hat von den Benutzern getrennte Einstellungen des Dateitypenfilters. Es können daher restriktive Einstellungen für die regulären Benutzer auf TightGate®-Pro Server wirksam sein und dennoch mittels ***transfer*** beliebige Dateien übertragen werden.
- Ein ***transfer***-Benutzer bleibt auch vom systemweiten Verbot der Nutzung der Dateischleuse unbehelligt und darf weiterhin Dateien über die Dateischleuse übertragen.
- Bei Bedarf können neben dem Benutzer ***transfer*** selbst bis zu 99 weitere ***transfer***-Benutzer durch den Administrator ***config*** aktiviert und anschließend über den Administrator ***maint*** individuell konfiguriert werden.
- Ein Systemverwalter kann sowohl einzelnen Benutzern den individuellen Dateitransfer freischalten als auch zusätzlich über den Benutzeraccount ***transfer*** tätig werden.

Warnung: Zum Erhalt der CC-Konformität ist es bei TightGate®-Pro (CC) Version 1.4 Server zwingend erforderlich, dass sich der mit einem ***transfer***-Benutzer agierende Rechner außerhalb des Klientennetzwerks befindet. Damit eine Verbindung mit TightGate®-Pro (CC) Version 1.4 Server dennoch erfolgen kann, muss die IPv4-Adresse dieses Rechners unter ***config > Einstellungen > Wartung und Updates > Nagios / Storage IP*** hinterlegt sein.

4.8 On-Access-Malware-Scanner

Die Dateischleuse von TightGate®-Pro Server kann durch Malware-Scanner serverseitig überwacht werden. TightGate®-Pro Server kann hierzu serienmäßig mit vorinstalliertem Malware-Scanner geliefert werden. Eine nachträgliche Installation ist ebenfalls möglich. In jedem Fall ist eine Lizenz einzuspielen, mit der der Malware-Scanner über den gebuchten Lizenzzeitraum aktualisiert werden kann. Der Ablauf der Lizenz wird über die Statusseite von TightGate®-Pro Server sowie über den entsprechenden Prüfpunkt der Nagios-Systemüberwachung angezeigt. Die Lizenz ist in diesem Fall zu erneuern, damit der Scanner weiterhin mit aktuellen Schadcode-Definitionen (Signaturen) versorgt wird.

Hinweis: TightGate®-Pro Server ist standardmäßig zur Verwendung mit den Malware-Scannern F-Prot und ESET Security. Die Verwendung alternativer Scanner ist unter bestimmten Voraussetzungen möglich. Nähere Auskünfte erteilt der technische Kundendienst der m-privacy GmbH.

Achtung: Der Malware-Scanner kann auch nach Lizenzablauf weiterverwendet werden, dessen Schutzwirkung ist jedoch eingeschränkt. Die Erkennungsleistung bezüglich aktueller Schadsoftware wird durch veraltete Definitionsdateien stark vermindert. Zum automatischen Bezug tagesaktueller Signaturen vom Hersteller der Software ist eine gültige Lizenz erforderlich.

4.8.1 Nachträgliche Installation eines Malware-Scanners

TightGate®-Pro Server kann mit werkseitig installiertem und lizenziertem Malware-Scanner geliefert werden. Sollte dies nicht der Fall sein, kann das Produkt bei Bedarf nachinstalliert werden. Dies geschieht in den folgenden Schritten:

1. Anmeldung als Administrator ***update***.
2. Installation des Pakets unter ***update > Kundendienst > Optionale Pakete zufügen***.

Die Installation des gewählten Malware-Scanners startet. Nach Abschluss der Installation wird wieder das Menü ***Kundendienst*** angezeigt. Es kann verlassen werden, sofern keine weiteren Teil-Updates erfolgen sollen.

Hinweis: Der Malware-Scanner ESET ist ab Betriebssystem-Kernversion 3.10 lauffähig.

4.8.2 Konfiguration des Malware-Scanners F-Prot

Die Konfiguration des Malware-Scanners erfolgt als Administrator ***config***. Folgende Einstellungen müssen vorgenommen bzw. geprüft werden:

config > Einstellungen		Hinweise		
Menüoption	**Beschreibung**	**C**	**E**	**F**
Malware-Scanner	Auszuwählen: F-Prot **Hinweis:** Zum Betrieb mit TightGate®-Pro Server werden die On-Access-Malware-Scanner F-Prot und ESET empfohlen. Unter bestimmten Voraussetzungen ist der Einsatz alternativer Produkte möglich. Nähere Auskünfte erteilt der technische Kundendienst.		**E1**	
F-Prot-Lizenz-schlüssel	An dieser Stelle ist der Lizenzschlüssel zu F-Prot zu hinterlegen. Dieser enthält wesentliche Lizenzinformationen und bestimmt die Laufzeit des Vertrags zum Bezug aktueller Schadcode-Definitionen (Signaturen). Der Lizenzschlüssel ist mit unterschiedlichen Leistungsumfängen beim technischen Kundendienst der m-privacy GmbH erhältlich.		**E4**	
F-Prot-Typ	Für den Einsatz auf einem Fileserver muss dieser Parameter auf 46 stehen, bei einem Mailserver auf 36. Standardwert: 46 **Hinweis:** Der Standardwert muss unter normalen Bedingungen nicht geändert werden, ist jedoch in jedem Fall erforderlich.		**E6**	
Malware-Scanner starten	Option zum Aktivieren bzw. Deaktivieren des serverseitigen Malware-Scanners. **Achtung:** Es empfiehlt sich, diese Option abschließend zu kontrollieren und ggf. korrekt zu setzen, um das System nicht versehentlich mit deaktiviertem Malware-Scanner zu betreiben. **Hinweis:** Die Statusseite, die unter ***http://localhost*** aus einem Browserfenster in TightGate®-Pro Server nach Freigabe abrufbar ist, zeigt an, ob der Malware-Scanner derzeit aktiv ist.		**E1**	

4.8.3 Konfiguration des Malware-Scanners ESET Security

Die Konfiguration des Malware-Scanners erfolgt als Administrator ***config***. Folgende Einstellungen müssen vorgenommen bzw. geprüft werden:

config > Einstellungen		**Hinweise**		
Menüoption	**Beschreibung**	**C**	**E**	**F**
Malware-Scanner	Auszuwählen: ESET **Hinweis:** Zum Betrieb mit TightGate®-Pro Server werden die On-Access-Malware-Scanner F-Prot und ESET empfohlen. Unter bestimmten Voraussetzungen ist der Einsatz alternativer Produkte möglich. Nähere Auskünfte erteilt der technische Kundendienst.		**E1**	
ESET-Benutzername	Es ist der Benutzername zu hinterlegen, der im Zuge der Registrierung beim Hersteller vergeben wird.		**E4**	
ESET-Passwort	Es ist das Passwort zu hinterlegen, der im Zuge der Registrierung beim Hersteller festgelegt wird.		**E4**	
ESET-Lizenz-Import	Die Lizenz für den Malware-Scanner wird in Form einer Lizenzdatei mit der Erweiterung *.lic erteilt und nachgewiesen. Diese Datei ist im Transferverzeichnis des Administrators ***config*** zu hinterlegen und kann über diese Menüoption ausgewählt und importiert werden.			
Malware-Scanner starten	Option zum Aktivieren bzw. Deaktivieren des serverseitigen Malware-Scanners. **Achtung:** Es empfiehlt sich, diese Option abschließend zu kontrollieren und ggf. korrekt zu setzen, um das System nicht versehentlich mit deaktiviertem Malware-Scanner zu betreiben. **Hinweis:** Die Statusseite, die unter ***http://localhost*** aus einem Browserfenster in TightGate®-Pro Server nach Freigabe abrufbar ist, zeigt an, ob der Malware-Scanner derzeit aktiv ist.		**E1**	

4.8.4 Schadcode-Definitionsdateien (Signaturen) manuell aktualisieren

Die Schadcode-Definitionsdateien oder Signaturen sind ein integraler Bestandteil eines Malware-Scanners. Für eine optimale Erkennungsleistung des Scanners müssen die Definitionsdateien stets auf dem neuesten Stand sein. TightGate®-Pro Server lädt die jeweils aktuellen Definitionen täglich direkt vom Update-Server des Herstellers, sodass sich ein manueller Eingriff in der Regel erübrigt und die Aktualisierung der Definitionsdateien nicht vergessen werden kann.

Hinweis: Die Programmdateien des Malware-Scanners werden zusammen mit der Aktualisierung der Systemsoftware von TightGate®-Pro Server auf den neuesten Stand gebracht. Ein vollständiger Update-Durchlauf aktualisiert damit auch immer die Antivirus-Applikation. Die erforderlichen Programmpakete werden über den Update-Server der m-privacy GmbH bereitgestellt.

Für den Fall, dass die Schadcode-Definitionen (Signaturen) manuell aktualisiert werden sollen, ist folgendermaßen zu verfahren:

1. Anmeldung als Administrator ***maint***.
2. Wahl der Menüoption maint > Malware-Scanner-Update. Die Schadcode-Definitionen werden aktualisiert.

Hinweis: Im Fehlerfall sind Netzwerkprobleme die häufigste Ursache, sodass der Aktualisierungsserver des Herstellers nicht erreichbar ist. Weiterhin ist eine gültige Lizenz für den Malware-Scanner erforder-

lich. Diese Fehlerquellen sollten vor einer Konsultation des technischen Kundendienstes geprüft werden.

4.8.5 Überprüfung der Aktualität von Schadcode-Definitionsdateien (Signaturen)

Im Sinne der allgemeinen Systemsicherheit sollten die Schadcode-Definitionsdateien von Zeit zu Zeit auf Aktualität geprüft werden. So werden Fehler im Aktualisierungsprozess zeitnah erkannt und können umgehend behoben werden.

Die Aktualitätsprüfung kann auf der Statusseite von TightGate®-Pro Server erfolgen, die nach Eingabe von ***http://localhost*** im Browser eines beliebigen Benutzers angezeigt wird. Je nach Einstellung ist ein Login mit dem Benutzer „status" und einem Kennwort erforderlich, das als Administrator ***config*** festgelegt werden kann.

Achtung: Sollte dieses Datum mehr als einen Tag vom aktuellen Tagesdatum abweichen, ist davon auszugehen, dass die automatische Aktualisierung der Definitionsdateien nicht korrekt erfolgt. Bis zur Behebung etwaiger Fehler empfiehlt es sich, die Signaturen manuell zu aktualisieren (siehe oben).

Alternativ kann der Status eines installierten Malware-Scanners als Administrator ***maint*** über die Menüoption ***maint > Malware-Scanner: Status*** überprüft werden. Diese Menüoption wird nur angezeigt, wenn ein Malware-Scanner installiert ist.

Hinweis: Über die Statusseite via http://localhost im Browserfenster von TightGate®-Pro Server kann auch geprüft werden, ob ein installierter Malware-Scanner aktiv ist.

4.9 Lizenzverwaltung

Um die von TightGate®-Pro Server bereitgestellten Dienste nutzen zu können, muss eine gültige Lizenz erworben und ordnungsgemäß im System hinterlegt werden. In Zweifelsfall unterstützt und berät der technische Kundendienst der m-privacy GmbH in allen Fragen zur Lizenzierung von TightGate®-Pro.

4.9.1 Einspielen der Lizenz

Der nachfolgende Prozess erfordert den Zugang zur Administrationsoberfläche von TightGate®-Pro Server als Administrator ***config***.

Die seitens der m-privacy GmbH erhältliche Lizenzdatei ist in das Transfer-Verzeichnis des Administrators ***config*** zu kopieren:

```
/home/config/transfer
```

Dies kann durch den Administrator ***config*** oder den Benutzer ***transfer*** über das mitgelieferte Schleusenprogramm erfolgen oder ein anderes Programm, welches das SFTP-Protokoll beherrscht.

Das eigentliche Einspielen der Lizenz erfolgt durch den Administrator ***config***. Bei Aufruf des Menüpunkts ***config > Lizenz importieren*** werden sämtliche Lizenzdateien angezeigt, die in oben angegebenem Verzeichnis hinterlegt wurden. Die benötigte Lizenzdatei ist auszuwählen und der Import mit ***OK*** zu bestätigen.

Achtung: Die Lizenz wird wirksam, nachdem im Hauptmenü ***config > Einstellungen*** die Option ***Sanft Anwenden*** gewählt wurde.

Hinweis: Bei Verbundrechnersystemen (Clustersystemen) müssen Lizenzdateien nur auf einem Rechner des Verbunds (Node) eingespielt werden. Die Verteilung der Lizenzen auf die übrigen Nodes des Clusters erfolgt im laufenden Betrieb automatisch. Es kann jeweils nur eine Lizenzdatei zur gleichen Zeit eingespielt werden.

4.9.2 Prüfung der Lizenzkapazität

Es besteht jederzeit die Möglichkeit, die Anzahl verfügbarer Lizenzen auszulesen. Als Administrator ***config*** kann die Lizenzdatei über den Menüpunkt ***config > Lizenzdatei anzeigen*** abgerufen werden. Weiterhin kann jeder VNC-Benutzer die Zahl verfügbarer Lizenzen über die Statusseite von TightGate®-

Pro Server über ***http://localhost/*** aufrufen. Je nach Voreinstellung ist die Eingabe von Zugangsdaten des virtuellen Benutzers ***status*** erforderlich.

Hinweise: Das Passwort für den virtuellen Benutzer ***status*** wird bei der Installation des Systems vergeben. Soll das Passwort geändert werden, geschieht dies als Administrator ***config*** über das Menü ***config > Einstellungen > Status: Passwort***. Falls kein Passwort vergeben wird, ist die Statusseite von jedem angemeldeten VNC-Benutzer über den Browser einsehbar. Veränderungen an Systemparametern können indessen nicht vorgenommen werden.

5 Benutzerverwaltung

Zur Benutzerverwaltung erfolgt die Anmeldung als Benutzer ***maint*** in der Konsole.

Hinweis: Die hier aufgeführten Einstellungen als Administrator ***maint*** betreffen einzelne Benutzer oder Benutzergruppen. Globale Einstellungen grundsätzlicher Natur werden durch den Administrator ***config*** in den jeweiligen Menüs vorgenommen, dort können auch Vorgaben für bestimmte Einstellungen gemacht werden.

maint		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Ende	Abmeldung vom System als Administrator ***maint.***		**E0**	
Benutzerverwaltung	Detaillierte Einstellungen bezüglich der Benutzer von TightGate®-Pro Server: Passworte, Quota, Benutzer anlegen und löschen, weitere benutzerorientierte Einstellungen. **Hinweise:** Benutzerkonten können auch aus einem Backup zurückgespielt werden. Bei erschöpfter Quota eines Benutzerkontos wird die Anmeldung des Benutzers von TightGate®-Pro Server abgewiesen.		**E1** **E2** **E3** **E4**	**F3**
Gruppenverwaltung	Einstellungen bezüglich Benutzergruppen. **Hinweise:** Es besteht weiterhin die Möglichkeit, Benutzergruppen mit besonderer Funktionalität anzulegen. Vgl. in diesem Zusammenhang den Abschnitt „Direktanmeldung in eine Administratorenrolle“. Gruppendefinitionen können auch aus einem Backup zurückgespielt werden.		**E1** **E4**	
Passwort-Optionen	Einstellungen zu Ablaufzeiten und Passwort-Historie.		**E2** **E6**	
Webseiten-Filter	Filteroptionen bezüglich URLs und Domänen.		**E1** **E4**	
Wartungs-Betrieb	Systemwartung bei Benutzern ankündigen bzw. absagen und TightGate®-Pro Server in den geplanten Wartungsbetrieb schalten. Sobald diese Option aktiviert ist, erhalten angemeldete Benutzer in regelmäßigen Abständen ein Hinweisfenster mit Informationen auf eine bevorstehende Systemwartung (Verbund: Beginn 50 Minuten vor der geplanten Wartung, Wiederholung alle 10 Minuten; Einzelsystem: Beginn 2 Stunden vor der geplanten Wartung, Wiederholung alle 30 Minuten). In einem Rechnerverbund (Cluster) wird der jeweilige Einzelrechner (Node) bereits eine Stunde vor dem Wartungstermin aus dem Cluster ausgekoppelt, sodass die automatische Lastverteilung keine weiteren Anmeldungen auf diesem Rechner mehr gestattet. Der Administrator kann angemeldete Benutzer zwangsweise abmelden. Im Fall von Änderungen, die den Abbruch laufender Benutzersitzungen zur Folge hätten, erhält der Administrator vor der Ausführung einen entsprechenden Warnhinweis.		**E1** **E2** **E4**	**F0** **F8**
VNC-Anmeldung aktivieren / deaktivieren	Wird diese Option gewählt, sind über bereits bestehende Verbindungen hinaus keine weiteren Anmeldungen an TightGate®-Pro Server möglich. Bestehende Verbindungen werden gehalten. Diese Option kann beispielsweise im Zusammenhang mit einer geplanten Systemwartung verwendet werden.		**E2**	

maint		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
GnuPG ID	Einstelloptionen im Zusammenhang mit einem zentralen GnuPG-Schlüssel. **Hinweis:** Diese Menüoption wird nur angezeigt, wenn ein zentraler GnuPG-Schlüssel hinterlegt wurde. Nähere Informationen erteilt der technische Kundendienst der m-privacy GmbH.		**E1 E2 E3 E4 E6**	**F3 F6**
Neustart	Einmaliger Reboot von TightGate®-Pro Server sofort oder zu einer bestimmten Uhrzeit.		**E2 E7**	**F7 F8**
Neustart abbrechen	Löschung eines geplanten Neustarts.		**E2**	
Herunterfahren	Kontrolliertes Herunterfahren und Abschalten von TightGate®-Pro Server.		**E2**	
Fernwartungsver-bindung auf	Öffnet einen Fernwartungstunnel zur Unterstützung durch den technischen Kundendienst der m-privacy GmbH. **Achtung:** Die Konfiguration des Fernwartungstunnels erfolgt durch den Administrator ***config***. **Warnung:** Unsachgemäße Konfiguration und Verwendung von Fernwartungszugängen können Betriebsstörungen hervorrufen und die Sicherheit von TightGate®-Pro Server sowie angeschlossener Netzwerke gefährden. Erforderlichenfalls sollte der technische Kundendienst der m-privacy GmbH konsultiert werden.		**E0**	**F0**
Fernwartungsver-bindung zu	Sofortige Unterbrechung der bestehenden Fernwartungsverbindung.		**E0**	**F0**
Fernwartungsverb. Status	Anzeige des Status' der Fernwartungsverbindung als „offen“ oder „geschlossen“.		**E0**	**F0**
SSH Admin auf	Öffnet für den begrenzten Zeitraum von einer Stunde einen SSH-Zugang für die Administratoren ***root*** oder ***security***. **Warnung:** Unsachgemäße Konfiguration und Verwendung von Fernwartungszugängen können Betriebsstörungen hervorrufen und die Sicherheit von TightGate®-Pro Server sowie angeschlossener Netzwerke gefährden. Erforderlichenfalls sollte der technische Kundendienst der m-privacy GmbH konsultiert werden.		**E0**	**F0**
SSH Admin zu	Weitere Anmeldungen als ***root*** oder ***security*** über SSH werden ab sofort nicht mehr zugelassen.		**E0**	**F0**
SSH Admin Status	Anzeige des Status der SSH-Admin-Zulassung. Es erfolgt eine Meldung, ob der Zugang offen oder geschlossen ist.		**E0**	**F0**
IPTraf	Diese Menüoption startet ein Programm zur detaillierten Netzwerkanalyse.			
Malware-Scanner: Status	Statusinformation des installierten Malware-Scanners. **Hinweis:** Wenn kein Malware-Scanner installiert und aktiviert ist, wird diese Menüoption nicht angezeigt.			
Malware-Scanner: Update	Aktualisierung der Schadcode-Definitionsdateien des installierten Malware-Scanners. Zum Bezug der Definitionsdateien vom Hersteller ist eine gültige Lizenz erforderlich. **Hinweis:** Wenn kein Malware-Scanner installiert und aktiviert ist, wird diese Menüoption nicht angezeigt.			
Maint-Passwort	Ändern des Zugangspassworts für den Administrator ***maint.*** **Hinweis:** Die Zugangskennung lautet immer „maint“ und kann nicht geändert werden.		**E2 E4**	

5.1 Benutzer anlegen und verwalten

In dieser Sektion können reguläre Benutzer angelegt, gelöscht, Passworte neu vergeben und die benutzerspezifischen Einstellungen geändert werden.

Für das Anlegen eines neuen Benutzers ist zumindest ein Benutzername notwendig. Vor- und Nachname sind optional. Das als ***maint*** vergebene Initialpasswort soll der Benutzer möglichst schon nach dem ersten Login ändern. Wenn die entsprechenden Passwort-Optionen voreingestellt sind, wird der Benutzer automatisch vom System aufgefordert, dieses innerhalb einer vorgegebenen Zeitspanne zu ändern. Das Anlegen von neuen Benutzern geschieht in der Benutzerverwaltung, welche im Folgenden erklärt wird.

Bei Cluster-Systemen gelten alle Benutzereinstellungen grundsätzlich für den gesamten Cluster.

maint > Benutzerverwaltung		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Zurück	Rückkehr zum Hauptmenü.		**E0**	**F0**
Ablaufende Zugänge	Anzeige aller abgelaufenen oder in den nächsten 30 Tagen ablaufenden Benutzerzugänge.		**E0**	**F0**
Ablaufende Passwörter	Anzeige aller abgelaufenen oder in den nächsten 30 Tagen ablaufenden Benutzer-Passwörter.		**E0**	**F0**
Quota-Engpässe	Anzeige von Konten mit knappem Festplattenspeicherplatz bzw. großer Zahl an Dateien. Diesbezügliche Kontingente können unter ***Benutzer ändern*** konfiguriert werden. **Hinweis:** Bei erschöpfter Quota eines Benutzerkontos wird die Anmeldung des Benutzers von TightGate®-Pro Server abgewiesen.		**E0**	**F0**
Exportiere Ablaufende	Nach Eingabe eines Zeitraums in Tagen werden alle Benutzerkonten, deren Zugang oder Passwort abläuft bzw. bereits abgelaufen ist, die Quota-Engpässe aufweisen oder deren Benutzer inaktiv waren, als Liste in die Datei expired.txt geschrieben und diese im Transfer-Verzeichnis des Administrators ***config*** abgelegt.		**E6**	**F6**
Angemeldete Benutzer	Zeigt eine Liste momentan angemeldeter Benutzer.		**E0**	
Benutzer ändern	Grundlegende, benutzerindividuelle Einstellungen. Auch das Passwort des Benutzers ***lpadmin*** für den CUPS-Dienst kann hier gesetzt werden. Weiterhin können über diese Menüoption die zulässigen Kontingente für Festplattenplatz und Dateianzahl festgelegt werden. Auch das Zurücksetzen von Profilen und Browser-Lesezeichen ist über diese Menüoption möglich. **Hinweis:** Über diese Menüoption kann auch festgestellt werden, ob und auf welchem Server der Benutzer angemeldet ist.		**E1** **E2** **E4** **E6**	**F6**
Neuer Benutzer	Die Eingabe eines Benutzernamens ist notwendige Voraussetzung zum Anlegen eines neuen Benutzers. Es können nur Benutzernamen mit Kleinbuchstaben angelegt werden. Auch die grundlegenden Voreinstellungen für die LXDE-Benutzeroberfläche können hier vorgenommen werden.		**E4** **E6**	**F6**
Importiere Benutzer	Hier können Benutzer über eine CSV-Datei importiert werden. Die Datei muss im Transferverzeichnis des Benutzers ***config*** liegen. Je nach Systemleistung ist für den Import ausreichend Verarbeitungszeit einzukalkulieren (> 60 Min. pro 1000 Benutzerkonten).		**E1**	

maint > Benutzerverwaltung		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Regeneriere Benutzer	Rücksicherung von Benutzerkonten aus einem Backup. Die Sicherungsdatei muss sich auf einer lokalen Partition oder einer angeschlossenen USB-Festplatte befinden.		**E1**	
Lösche Benutzer	Entfernen von Benutzern aus dem System und Löschung aller Daten des Benutzers (Löschung des Home-Verzeichnisses und aller abgespeicherten Daten).		**E1** **E2**	
Inaktive Benutzer	Über diesen Menüpunkt können Benutzer, die über einen bestimmten Zeitraum nicht angemeldet waren, angezeigt und ggf. gelöscht werden. Der Zeitraum in Tagen der Inaktivität ist wählbar.		**E1** **E2** **E6**	**F6**
Datei-Transfer	Erlaubnis für einzelne Benutzer oder Benutzergruppen, den Dateitransfer verwenden zu dürfen. Mit der Freischaltung des Dateitransfers steht dem jeweiligen Benutzer bzw. den Mitgliedern freigegebener Gruppen die Möglichkeit offen, Daten über das SFTP-Protokoll (z. B. über das seitens der m-privacy GmbH erhältliche Schleusen-Programm) zu transferieren. Die Übertragung kann auf bestimmte Dateitypen beschränkt werden. **Hinweis:** Für Transfer-Benutzer (ein einzelner oder mehrere) kann diese Erlaubnis nicht bearbeitet werden. Transfer-Benutzer können per definitionem stets alle MIME-Typen übertragen.		**E1**	
Gefiltertes Web	Auswahl derjenigen Benutzer oder Benutzergruppen, die den Inhaltsfilter-Proxy auf TightGate®-Pro Server umgehen dürfen. Diese Benutzer bzw. die Mitglieder freigegebener Gruppen erhalten vollen Zugriff auf das Internet ohne inhaltliche Einschränkungen. Die Einstellung des Inhaltsfilters selbst kann nur vom Administrator ***config*** vorgenommen werden.		**E1**	
Audio-Unterstützung	Berechtigung für einzelne Benutzer zur Audio-Übertragung vom TightGate®-Pro Server-System zum Klienten. **Achtung:** Zur Nutzung der Audio-Dienste sind neben dieser Einstellung noch weitere Voraussetzungen am Arbeitsplatzrechner und ggf. an einer zwischengeschalteten Firewall zu erfüllen. Wird die Audio-Wiedergabe eingeschaltet, ist dann jedoch aufgrund weiterer Randbedingungen im Netzwerk nicht möglich, kommt es zu starken Beeinträchtigungen der Videowiedergabe. Im Zweifelsfall sollte die Einstellung „Testen“ aktiviert oder die Audiowiedergabe bewusst abgeschaltet werden.		**E1**	

maint > Benutzerverwaltung		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Privilegierter Zugang	Auswahl der Benutzer oder Benutzergruppen, die einen bevorrechtigten Zugang zu TightGate®-Pro Server erhalten sollen. **Hinweis:** TightGate®-Pro Server unterscheidet zwei Grenzen, bis zu denen Benutzeranmeldungen zugelassen werden. Diese werden in der Lizenz zu TightGate®-Pro hinterlegt und sind ausschließlich durch den technischen Kundendienst der m-privacy GmbH veränderbar. Die erste Grenze bezeichnet die Zahl regulärer Benutzer, die zweite Grenze bezeichnet die Zahl der privilegierten Benutzer. Sobald die Zahl zulässiger regulärer Nutzer erreicht ist, werden nur noch privilegierte Nutzer zugelassen - vorausgesetzt, deren Zahl ist noch nicht erreicht. Nach Ausschöpfung der zweiten Grenze wird jeder weitere Verbindungsversuch eines Klienten an TightGate®-Pro Server mit einer entsprechenden Fehlermeldung abgewiesen. Privilegierte Klienten werden nicht nur entsprechend eines gesonderten Kontingents zugelassen, sondern darüber hinaus mit einem größeren Anteil an Arbeits- und Massenspeicher sowie CPU-Zeit auf TightGate®-Pro Server ausgestattet.		**E1**	
Drucken in Spool	Legt fest, ob ein Benutzer direkt auf den Drucker oder in das Spool-Verzeichnis auf TightGate®-Pro ausdruckt. **Hinweis:** Im letzteren Fall ist zur weiteren Verarbeitung die entsprechende Klientensoftware zur Spool-Verarbeitung auf den Klienten-Rechnern erforderlich, da andernfalls keine Druckausgabe erfolgen kann.		**E1** **E2**	
Auto-Zwischenablage	Auswahl der Benutzer oder Benutzergruppen, für die die Nutzung der Zwischenablage gestattet werden soll. **Hinweis:** Ist die Nutzung der Zwischenablage durch ***config*** systemweit abgeschaltet, bleibt diese Option ohne Wirkung.		**E1**	
Typ / Profil ändern	Auswahl zwischen der standardmäßigen Benutzerschablone und einer kundenspezifischen Benutzerschblone (falls definiert). **Hinweis:** Eine kundenspezifische Benutzschablone kann nur über den technischen Kundendienst der m-privacy GmbH definiert werden.		**E1**	
LXDE-Optionen	Benutzer- oder gruppenspezifische Einstellmöglichkeiten der verfügbaren Optionen der LXDE-Oberfläche für bestehende Benutzer. **Hinweis:** Die LXDE-Optionen für neu angelegte Benutzer oder solche, die im Zuge einer Anmeldung via Active Directory automatisch angelegt werden, werden entsprechend der geltenden Benutzerprofil-Vorgabe durch den Administrator ***config*** festgelegt. **Achtung:** Werden die LXDE-Optionen für Benutzerkonten mit dem Profil „Custom“ an dieser Stelle manuell geändert, fällt die Konfiguration der Menüleiste generell auf Standardwerte für das jeweilige Profil zurück. Der technische Kundendienst der m-privacy GmbH bietet daher Unterstützung für den Fall, dass kundenspezifische Benutzerprofile weitergehend angepasst werden müssen.		**E1**	
Maximale Dateigröße	Festlegung der maximalen Dateigröße, die über die Dateischleuse transferierbar sein soll. Der eingegebene Wert gilt in beide Richtungen. Werte über 4296 MB können im Rahmen einer kundenspezifischen Beuntzerschablone über den technischen Kundendienst der m-privacy GmbH eingestellt werden.		**E6**	**F6**

maint > Benutzerverwaltung		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Benutzer-Sprache	Auswahl der Benutzersprache, nutzerindividuell oder gruppenbezogen.		**E1** **E2**	
Profil zurücksetzen	Auswahl der Benutzer oder Benutzergruppen, deren Profil auf Standardwerte zurückgesetzt werden soll. **Hinweis:** Bevor das Profil eines angemeldeten Benutzers zurückgesetzt wird, erfolgt eine Sicherheitsabfrage. Bei positiver Bestätigung wird der Benutzer von TightGate®-Pro Server getrennt und dessen Profil zurückgesetzt.		**E1** **E2**	
Lesezeichen zurücksetzen	Sollten sich aufgrund eines Dateifehlers die Lesezeichen eines Benutzers nicht mehr verwenden lassen, können sie mit dieser Menüoption durch die Standard-Lesezeichen der Profilvorgabe ersetzt werden. Anschließend können weitere Lesezeichen neu angelegt oder aus einem Backup (Datensicherung) zurückgespielt werden, sofern vorhanden.		**E0** **E1** **E2**	
Prozesse lokal beenden	Auswahl einer Benutzerkennung, deren laufende Prozesse sämtlich beendet werden sollen. Der Benutzer wird dabei stets abgemeldet. Es werden nur angemeldete Benutzer gezeigt. Im Rechnerverbund bezieht sich die Anzeige nur auf den Knoten (Node), an dem sich der Administrator ***maint*** angemeldet hat. Diese Funktion dient als Notbehelf, falls ein Benutzer Applikationen nicht mehr starten oder schließen kann. Im Bedarfsfall kann ein Knoten im Rechnerverbund von allen Benutzern geräumt werden. **Warnung:** Diese Funktion sollte nur nach Rücksprache mit den betroffenen Benutzern verwendet werden, da unter Umständen Daten verloren gehen können.		**E1** **E2**	
Prozesse Cluster beenden*	Auswahl einer Benutzerkennung aus dem gesamten Rechnerverbund (Cluster), deren laufende Prozesse sämtlich beendet werden sollen. Der Benutzer wird dabei stets abgemeldet. Es werden nur angemeldete Benutzer gezeigt. Diese Funktion dient als Notbehelf, falls ein Benutzer Applikationen nicht mehr starten oder schließen kann. **Warnung:** Diese Funktion sollte nur nach Rücksprache mit den betroffenen Benutzern verwendet werden, da unter Umständen Daten verloren gehen können.		**E1** **E2**	

maint > Benutzerverwaltung		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Massen-SSL-Schlüssel	Ein Assistent erzeugt eine beliebige Anzahl von SSL-Zertifikaten zur SSO-Anmeldung an TightGate®-Pro Server im Voraus. Diese können auf Arbeitsplatzstationen verteilt werden und ermöglichen in Verbindung mit dem passenden Viewer und dem Schleusenprogramm der m-privacy GmbH eine zertifikatsbasierte Anmeldung an TightGate®-Pro Server. Es kann ein beliebiges Präfix vorgegeben werden, fortlaufende Kennungen werden automatisch ergänzt. Die Zertifikate tragen stets vier Ziffern im Benutzernamen. **Hinweis:** Die erzeugten Zertifikate müssen mit der Option Export. SSL-Schlüssel exportiert werden. Erst dann befinden sie sich im Transferverzeichnis des Administrators ***config*** (/home/config/transfer). Sie können dort per SFTP abgeholt und auf die Arbeitsplatzrechner verteilt werden. **Achtung:** Diese Option beinhaltet nicht das Anlegen der zugehörigen Benutzerkonten, ohne die eine Anmeldung auch mit gültigem Zertifikat nicht möglich ist. Diese müssen entweder manuell oder nach expliziter Konfiguration über TightGate®-Pro Server automatisch generiert werden. Hierzu bestehen mehrere Optionen. Die notwendigen Einstelloptionen können als Administrator ***config*** global in den ***Einstellungen*** gewählt werden.		**E4** **E6**	**F6**
Erzeuge SSL-Schlüssel	Diese Option erzeugt SSL-Zertifikate zum Single Sign-on an TightGate®-Pro Server für bereits bestehende Benutzerkonten oder für die Mitglieder von Benutzergruppen. **Hinweis:** Die erzeugten Zertifikate befinden sie sich im Transferverzeichnis des Administrators ***config***. (/home/config/transfer). Sie können dort per SFTP abgeholt und auf die Arbeitsplatzrechner verteilt werden.		**E1**	
Export. SSL-Schlüssel	Auswahl und Export generierter Zertifikate zu bestehenden Benutzerkonten. Diese befinden sich anschließend im Transferverzeichnis des Administrators ***config***. Sie können dort per SFTP abgeholt und auf die Arbeitsplatzrechner verteilt werden.		**E1**	
Rückruf Zertifikat	Zertifikate, die nicht länger benötigt werden oder ungültig sein sollen, können mit dieser Option widerrufen werden. Es werden nur Benutzer angezeigt, die über ein Zertifikat zum Single Sign-on verfügen. **Hinweis:** Ein einmal widerrufenes Zertifikat kann nicht mehr reaktiviert werden. Wird für die betreffende Benutzerkennung erneut ein SSL-Zertifikat benötigt, ist ein solches neu auszustellen, zu exportieren und zu verteilen.		**E1** **E2**	

Hinweis: Alle Einstellungen werden ohne Neustart sofort wirksam. ***Sanft Anwenden*** ist nicht notwendig.

5.2 Benutzergruppen anlegen und verwalten

Benutzergruppen rationalisieren die Verwaltung von Benutzern mit gemeinsamen Einstellungen bzw. Berechtigungen. Auf TightGate®-Pro Server können beliebige Gruppen definiert und anschließend einzelne Benutzer diesen Gruppen zugeordnet werden. Beispiel für eine Gruppe wäre z.B. die Gruppe ***schleuse***, in der alle Benutzer mit speziellen Datei-Transferberechtigungen zusammengefasst werden. Die Arbeit mit Benutzergruppen erfolgt als Administrator ***maint*** unter dem Menüpunkt ***Gruppenverwaltung***.

Achtung: Benutzergruppen auf TightGate®-Pro Server dienen nur der zeitgleichen Konfiguration mehrerer Benutzerkonten, hierüber vorgenommene Einstellungen werden immer auf die einzelnen Benutzerkonten übertragen. Benutzergruppen wirken nicht als Schablonen für Berechtigungssätze, die an die Gruppeneigenschaft gebunden sind. Dies bedeutet beispielsweise, dass über eine Gruppe erteilte Berechtigungen bei den betreffenden Benutzerkonten erhalten bleiben, auch wenn die Gruppe anschließend gelöscht wird. Gruppenberechtigungen können durch eine nachfolgende Einzelkonfiguration überschrieben werden und umgekehrt. Grundsätzlich hat die jeweils letzte Konfiguration eines Benutzerkontos Bestand, unabhängig vom Weg der Einstellung. Es empfiehlt sich daher eine abgestufte Verfahrensweise von systemweiten Einstellungen über Gruppeneinstellungen hin zur Einzelkonfiguration von Benutzerkonten, um Konfigurationsfehler zu vermeiden.

In folgenden Schritten wird eine neue Gruppe angelegt, ein Benutzer hinzugefügt sowie der Gruppe ein spezielles Recht vergeben.

3. Gruppe anlegen und Gruppenname vergeben erfolgt mittels ***Gruppenverwaltung > Neue Gruppe***. Wird eine Gruppe nicht mehr benötigt, kann sie mit dem Menüpunkt ***Gruppe entfernen*** gelöscht werden.

   Achtung: Nach dem Löschen einer Gruppe bleiben eventuell durch die Gruppenberechtigungen auf die enthaltenen Benutzerkonten erhalten! Ist dieses Verhalten unerwünscht, sollten die Berechtigungen zunächst in der Gruppe für alle inkludierten Benutzerkonten wunschgemäß geändert werden, bevor die Gruppe gelöscht wird.

4. Benutzer hinzufügen: Über den Menüpunkt ***Benutzer in Gruppe*** - es können beliebig viele Benutzer zu einer Gruppe hinzugefügt werden. Auch der umgekehrte Weg kann über den Menüpunkt ***Gruppe zu Benutzer*** beschritten werden.

5. Rechte zuweisen: Sind die Benutzer den Gruppen zugeordnet, können der Gruppe (und damit allen ihr zugehörigen Benutzern) nach Wunsch Rechte zugeteilt werden. Hierzu besteht in den meisten Menüoptionen, in denen sich die Eigenschaften einzelner Benutzerkonten bearbeiten lassen, die Möglichkeit der Bearbeitung von Benutzergruppen.

Hinweis: Alle Einstellungen werden ohne Neustart sofort wirksam. ***Sanft Anwenden*** ist nicht erforderlich.

5.3 Direktanmeldung mit einer Administratorenrolle

Gelegentlich ist es wünschenswert, dass sich normale Benutzer an der Konsole oder per SSH als Administratoren anmelden können. Dies kann erforderlich sein, wenn mehrere Personen als Administrator tätig sind, das zentrale Passwort einer bestimmten Administratorenrolle in verteilten Organisationsstrukturen jedoch nicht einem größeren Personenkreis zugänglich gemacht werden soll. Sofern ein Benutzer einer bestimmten, eigens dafür vorgesehenen Benutzergruppe auf TightGate®-Pro Server angehört, kann dieser sich unmittelbar mit seinem regulären Passwort anmelden und erhält automatisch die Privilegien der jeweiligen Administratorenrolle.

Zu diesem Zweck muss der Administrator ***maint*** zunächst die notwendigen, speziellen Gruppen in der Gruppenverwaltung von TightGate®-Pro Server anlegen. Diese Gruppen müssen, entsprechend ihrer Zweckbestimmung, zwingend die folgenden Bezeichnungen beginnend mit „tgadmin“ tragen:

Gruppe	Beschreibung
tgadmin***config***	Gruppenmitglieder können als Administrator ***config*** agieren.
tgadmin***maint***	Gruppenmitglieder können als Administrator ***maint*** agieren. Ausnahme: Gruppenmitglieder können keine Gruppen zur Direktanmeldung mit einer Administratorenrolle anlegen oder ändern (z. B. Benutzer entfernen oder hinzufügen, tgadmin-Gruppen anlegen oder löschen).
tgadmin***update***	Gruppenmitglieder können als Administrator ***update*** agieren.

tgadmin***backuser***	Gruppenmitglieder können als Administrator ***backuser*** agieren.
tgadmin***security***	Gruppenmitglieder können als Administrator ***security*** agieren.
tgadmin***root***	Gruppenmitglieder können als Administrator ***root*** agieren.

Alle Benutzerkennungen, die auch zu einer Anmeldung mit einer Administratorenrolle berechtigt sein sollen, sind den jeweiligen Gruppen hinzuzufügen. Dies darf ausschließlich der tatsächliche Administrator ***maint*** bewerkstelligen, nicht etwa ein Mitglied der bestehenden Gruppe tgadmin***maint***.

Anschließend kann sich der Benutzer mit allen Administratorenrollen anmelden, die durch seine Zugehörigkeit zu den jeweiligen tgadmin-Gruppen festgelegt sind. Statt seiner Benutzerkennung ***benutzer*** allein wird beim Login-Prompt eine Kennung nach dem Schema ***benutzer+adminrolle*** angegeben, beispielsweise also ***testbenutzer+maint***. Das zu verwendende Passwort entspricht dem regulären Passwort des Benutzers. Das Passwort der eigentlichen Administratorenrolle ***adminrolle*** ist zur Anmeldung eines regulären Benutzers nicht erforderlich.

Hinweis: Die Zugriffe eines auf diese Weise mit erhöhten Privilegien angemeldeten Benutzers werden protokolliert.

Mit einer Administratorenrolle angemeldete Benutzer erhalten alle wesentlichen Privilegien der betreffenden Administratorenrolle.

5.4 Passwortoptionen

Die Menüfunktion ***Passwort-Optionen*** steht dem Administrator ***maint*** im Hauptmenü zu Verfügung. Sie erlaubt Regelungen zum Gebrauch von Passwörtern und Zugangsberechtigungen, sofern die interne Benutzerverwaltung von TightGate®-Pro Server verwendet wird. Das Initialpasswort eines neuen Benutzers ist nicht an die Mindestvorgaben für Passwörter gebunden, es kann beispielsweise einfacher zusammengesetzt sein.

Warnung: Es sollte im Interesse der allgemeinen Systemsicherheit darauf geachtet werden, dass Benutzer möglichst bereits beim ersten Anmelden zu einer Passwortänderung aufgefordert werden, falls ein einfaches Initialpasswort gesetzt wurde. Der Menüpunkt ***Initiale Ablaufzeit*** gestattet die Festlegung des Zeitraums, über den das Initialpasswort höchstens gelten soll.

maint > Passwort-Optionen		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Zurück	Rückkehr zum Hauptmenü.		**E0**	
Speichern	Speichern und Anwenden der neuen Einstellungen auf bestehende Benutzer sowie Setzen dieser Einstellungen als Voreinstellungen für neue Benutzer.		**E2**	
Initiale Ablaufzeit	Gibt an, nach wie vielen Tagen das Initialpasswort geändert werden muss. Wird das Initialpasswort nicht innerhalb der festgelegten Zeit geändert, so wird der Benutzerzugang gesperrt und es muss ein neues Initialpasswort durch ***maint*** vergeben werden.		**E6**	**F6**
Ablaufzeit	Gültigkeitsdauer eines regulären Passwortes. Nach Ablauf der eingestellten Zeitspanne muss der Benutzer sein Passwort ändern, bevor eine Anmeldung an TightGate®-Pro Server erfolgt.		**E6**	**F6**
Min. Ablaufzeit	Mindestgültigkeit für Passwörter. Eine Änderung vor Ablauf dieser Frist ist nicht möglich. Standardwert ist 0 Tage.		**E6**	**F6**
Warn-Periode	Gibt an, wie viele Tage vor Ablauf eines Passwortes Benutzer einen Hinweis erhalten, dass das Passwort in Kürze ungültig wird. Der Hinweis zur Änderung des Passworts wird bei jeder Anmeldung ausgegeben.		**E6**	**F6**

maint > Passwort-Optionen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Min. Pass-wort-Länge	Festlegung der Mindestlänge für Benutzerpasswörter. Kürzere Passwörter als hier angegeben werden vom System nicht akzeptiert. **Warnung:** Im Sinne der grundlegenden Sicherheit von Passwörtern sollte ein Passwort mindestens sechs Zeichen lang sein. Die Voreinstellung beträgt 8 Zeichen. **Achtung:** Das Initialpasswort, das vom Administrator ***maint*** vergeben wird, kann als einzige Ausnahme kürzer sein. Es ist darauf zu achten, eine sinnvolle ***Initiale Ablaufzeit*** zu wählen und Benutzer somit zeitnah zur Änderung des Initialpassworts aufzufordern.		**E6**	**F6**
Passwort-Historie	TightGate®-Pro Server verhindert die erneute Verwendung bereits abgelaufener Passworte in der hier angegebenen Tiefe. Versucht ein Benutzer, ein bereits verwendetes Passwort erneut zu setzen, obwohl es noch in der Passwort-Historie enthalten ist, wird das Passwort mit einer Fehlermeldung abgelehnt.		**E6**	**F6**

Achtung: Nachdem alle Änderungen an den Passwort-Optionen vorgenommen wurden, müssen diese über den Menüpunkt ***Speichern*** gesichert werden. Damit werden die neuen Einstellungen auf alle bestehenden und zukünftigen Benutzer angewendet. ***Sanft Anwenden*** ist nicht erforderlich.

5.5 Benutzer importieren

TightGate®-Pro Server kann Benutzerangaben aus einer vordefinierten Liste importieren. Den Benutzern können dabei verschiedene Merkmale übergeben werden. Die Importfunktion ist nur zur Datenübernahme für neue Benutzerkonten geeignet. Merkmale bestehender Benutzerkonten können über den Listenimport nicht verändert werden.

5.5.1 Import von Benutzern über eine Liste

Vorgehensweise:

1. Spezifikationsgerechte Liste mit Benutzerangaben bereitstellen (vgl. folgender Abschnitt)
2. Hinterlegung der Liste per Dateischleuse mit dem Administrator ***config*** in das Verzeichnis /home/config/transfer. Bei CC-Systemen erfolgt die Übertragung als Benutzer ***transfer***.
3. Anmeldung am TightGate®-Pro Server als Administrator ***maint***,
   Auswahl von ***Benutzerverwaltung > Importiere Benutzer***.
4. Auswahl einer CSV-Datei, aus der die Benutzerangaben importiert werden sollen.
5. Die Benutzerangaben werden importiert. Dabei entstehen neue Benutzerkonten. Nach Abschluss des Imports erfolgt eine Zusammenfassung über importierte Benutzerdaten, nicht importierte Benutzerdaten und aufgetretene Fehler.

Hinweis: Alle Änderungen sind nach dem Import sofort wirksam. Neue Benutzer können sich unmittelbar anmelden. Bei Cluster-Systemen kann eine kurze Wartezeit bis zu 10 Minuten erforderlich sein, bis die Benutzerkonten auf alle Knoten verteilt wurden.

5.5.2 Spezifikation der Liste für den Import

Eine Liste für den Benutzerimport in TightGate®-Pro Server muss folgende Anforderungen erfüllen:

- Die CSV-Datei muss die Endung .csv haben
- Trennzeichen der Felder in der CSV-Datei ist das Semikolon (;)
- Zeichenkette, z.B. Namen, in der CSV-Datei werden durch Anführungszeichen (”) abgegrenzt, Zahlenwerte werden ohne Anführungszeichen angegeben

- Die CSV-Datei darf keine Tabellenüberschrift enthalten
- Es sind in der CSV-Datei keine Umlaute (öäüß) oder Sonderzeichen (,.-;:_'`´) erlaubt

Die CSV-Datei hat folgenden schematischen Aufbau:

Benutzername	Klarname	Passwort	Dateitransfer	Gefiltertes Web	Sound	Clipboard	Profil
			0 = verboten 1 = erlaubt	0 = gefiltert 1 = ungefiltert	0 = ein 1 = an	0 = verboten 1 = erlaubt	0 = Standard 3 = Custom 5 = OEM

Eine Zeile aus einer CSV-Datei könnte demnach folgendermaßen aussehen:

```
"eka1";"Erika Mustermann";"geheim";0;0;0;0
```

Alle Einstellungen bezüglich der LXDE-Vorgaben werden aus den Voreinstellungen des Administrators ***Config*** automatisch übernommen. Eine Änderung ist nur nachträglich über die Benutzerverwaltung möglich.

Hinweis: Es werden nur neue Benutzer anhand des Benutzernamens importiert. Werte bestehender Benutzerkonten werden übersprungen und weder aktualisiert noch verändert. Nach dem Import wird eine Zusammenfassung mit Ergebnisbilanz auf dem Bildschirm angezeigt.

6 Installation und Konfiguration der TightGate®-Pro-Klientensoftware

Die Installation der Klientensoftware TightGate®-Viewer (TightGate®-Pro Client) und TightGate®-Schleuse erfolgt direkt an den Arbeitsplätzen. Die Applikationen für Linux- und Windows-Betriebssysteme können aus dem Support-Bereich der Internetpräsenz der m-privacy GmbH lizenzkostenfrei bezogen werden. Die einzelnen Installationsschritte unter Windows und unter Linux werden in den nächsten Abschnitten erläutert.

6.1 Verfügbare Programmpakete

Die notwendigen Programmpakete stehen im Support-Bereich der m-privacy-Internetpräsenz lizenzkostenfrei zum Abruf zur Verfügung.

Die teilautomatische Linkweiche MagicURL ist ebenfalls als installierbares Programmpaket im Support-Bereich der m-privacy-Internetpräsenz verfügbar. Es kann nur auf Klientenrechnern mit Windows®-Betriebssystem installiert werden.

Hinweise: TightGate®-Pro implementiert generell die Vollverschlüsselung des Dateitransfers sowie der VNC-Bildübertragung zwischen dem ReCoB-System (Server) und dem Arbeitsplatzrechner (Klient). Dabei kommt eine starke Verschlüsselung zum Einsatz, die standardmäßig für bestimmte, ältere Klienten-Konfigurationen insbesondere unter Windows® XP abgeschwächt wird, um Verbindungsprobleme zu vermeiden. Entsprechende Einstellungen auf TightGate®-Pro Server sind als Administrator ***config*** unter ***config > Einstellungen > Authentisierung*** vorzunehmen.

Die CC-konforme Variante der Viewer-Software TightGate®-Pro (CC) Version 1.4 Client erlaubt in der Werkseinstellung ausschließlich die Nutzung der Zwischenablage per Einzelbestätigung, der Verbindungsaufbau zum Server erfolgt immer TLS-verschlüsselt.

Weitere Hinweise zur Verschlüsselung der Kommunikation zwischen TightGate®-Pro Server und TightGate®-Pro Client auf den Arbeitsplatzrechnern erteilt auf Anfrage der technische Kundendienst der m-privacy GmbH.

Achtung: Es kann zum Betrieb mit TightGate®-Pro Server und TightGate®-Pro (CC) Version 1.4 Server ausschließlich der TightGate®-Viewer (TightGate®-Pro Client) verwendet werden, der seitens der m-privacy GmbH bereitgestellt wird. Bei jedem Versionswechsel des TightGate®-Viewers ist es bei der Verwendung eigener Zertifikate zum Single Sign-on (SSO) weiterhin zwingend erforderlich, diese auf TightGate®-Pro Server neu zu generieren und auf den Klientenrechnern einzuspielen.

Warnung: Die Audio-Übertragung zwischen TightGate®-Pro Server und den Klientenrechnern erfolgt stets unverschlüsselt. Daher eignet sich das System explizit nicht zur Übertragung vertraulicher Audio-Inhalte.

TightGate®-Viewer für Standardumgebungen	
VNC-Viewer für Windows XP (32 / 64 Bit) Windows 7 (32 / 64 Bit) Windows 8 (32 / 64 Bit) **Achtung:** Der TightGate®-Viewer zur Nutzung von TightGate®-Pro in Verbindung mit einem Active Directory ist unter Windows XP nicht lauffähig.	Der TightGate®-Viewer für Windows-Betriebssysteme ist als universelles Programmpaket sowohl auf 32- als auch auf 64-Bit-Systemen lauffähig. Es ist für alle verfügbaren Arten der Klientenauthentifizierung geeignet. Dieses Programm wird auf jedem Rechner benötigt, der die Bildschirmausgabe eines TightGate®-Pro-Servers anzeigen soll. Der TightGate®-Viewer steht in einer Version mit und in einer Version ohne eingebauten Druckspooler zur Verfügung. Er kann lizenzkostenfrei auf beliebig vielen Arbeitsplatzstationen installiert werden. **Achtung:** Die Anzahl gleichzeitig zugelassener Verbindungen ist abhängig von der für TightGate®-Pro gültigen Lizenz.

TightGate®-Viewer für Standardumgebungen	
TightGate®-Viewer für Debian GNU/Linux	Der TightGate®-Viewer steht für Debian, Ubuntu und andere auf der Paketverwaltung dpkg aufbauende Distributionen bereit. Er ist für alle verfügbaren Arten der Klientenauthentifizierung geeignet und kann lizenzkostenfrei auf beliebig vielen Arbeitsplatzstationen installiert werden. **Achtung:** Die Anzahl gleichzeitig zugelassener Verbindungen ist abhängig von der für TightGate®-Pro gültigen Lizenz.
TightGate®-Viewer für Apple OS X ab Version 10.9 (Mavericks)	Der TightGate®-Viewer steht für Apple OS X ab Version 10.9 Mavericks bereit. Er ist für alle verfügbaren Arten der Klientenauthentifizierung geeignet und kann lizenzkostenfrei auf beliebig vielen Arbeitsplatzstationen installiert werden. **Achtung:** Die Anzahl gleichzeitig zugelassener Verbindungen ist abhängig von der für TightGate®-Pro gültigen Lizenz.

TightGate®-Viewer für CC-konforme Umgebungen	
TightGate®-Pro (CC) Version 1.4 Client für Windows XP (32 / 64 Bit) Windows 7 (32 / 64 Bit) Windows 8 (32 / 64 Bit)	Der TightGate®-Viewer ist sowohl auf 32- als auch auf 64-Bit-Systemen lauffähig. Dieses Programm wird auf jedem Rechner benötigt, der die Bildschirmausgabe eines TightGate®-Pro-Servers anzeigen soll. Es kann lizenzkostenfrei auf beliebig vielen Arbeitsplatzstationen installiert werden und ist zur Anmeldung mit Zugangsdaten (Benutzername und Passwort) geeignet. Zur Anmeldung an TightGate®-Pro Server per Single Sign-on (SSO) kann auf den SSO-fähigen Viewer für Standardumgebungen zurückgegriffen werden, ohne dass die CC-Konformität infrage steht. **Achtung:** Die Anzahl gleichzeitig zugelassener Verbindungen ist abhängig von der für TightGate®-Pro gültigen Lizenz. TightGate®-Pro (CC) Version 1.4 Client ist nicht per Download verfügbar. Bitte wenden Sie sich an den technischen Kundendienst der m-privacy GmbH.

TightGate®-Schleuse, die Dateischleuse von TightGate®-Pro Server ist nutzerindividuell konfigurierbar. Weiterhin können Dateien über den zentralen Dateischleusen-Benutzer ***transfer*** ausgetauscht werden. ***transfer*** ist ein unveränderlicher Systembenutzer in TightGate®-Pro Server, dessen einzige Aufgabe die globale Durchführung von Dateitransfers über die Dateischleuse ist. Beide Varianten können parallel genutzt werden.

Die Dateischleuse kann von einem serverseitig operierenden Malware-Scanner geschützt werden, falls ein solcher installiert und lizenziert ist. Der Malware-Scanner blockiert Dateien in der Dateischleuse, falls diese virenbehaftet sind. Die Dateien können dann durch den Benutzer nicht transferiert, wohl aber gelöscht werden.

TightGate®-Schleuse (Schleusenprogramm)	
TightGate®-Schleuse für Windows XP (32 / 64 Bit) Windows 7 (32 / 64 Bit) Windows 8 (32 / 64 Bit) **Achtung:** Die TightGate®-Schleuse zum Datentransfer in Verbindung mit einem Active Directory ist unter Windows XP nicht lauffähig.	TightGate®-Schleuse ist sowohl auf 32- als auch auf 64-Bit-Systemen lauffähig. Je nach vorgesehener Authentifizierungsmethode ist das Schleusenprogramm zur Anmeldung mit Zugangsdaten oder zur Anmeldung per Single Sign-on (SSO) mit der jeweiligen Authentisierungsmethode auszuwählen. Dieses Programm wird auf jedem Rechner benötigt, auf dem der Dateitransfer mit TightGate®-Pro Server stattfinden soll. Es kann lizenzkostenfrei auf beliebig vielen Arbeitsplatzstationen installiert werden. **Hinweis:** Die Anzahl gleichzeitig zugelassener Verbindungen ist unabhängig von der für TightGate®-Pro gültigen Lizenz.

TightGate®-Schleuse (Schleusenprogramm)	
Schleusenprogramm für Linux-Derivate	Es eignet sich ein beliebiges Programm zur Dateiübertragung nach dem SFTP-Protokoll.
Schleusenprogramm für Apple OS X	Es eignet sich ein beliebiges Programm zur Dateiübertragung nach dem SFTP-Protokoll. Wir empfehlen die Freeware *Cyberduck*, da sich damit auch die zertifikatsbasierte Anmeldung (Single Sign-on) einrichten lässt.

6.2 TightGate®-Viewer unter Microsoft® Windows®

6.2.1 Installation

Die über den Support-Bereich der Internetpräsenz der m-privacy GmbH bereitgestellten Installationsdateien sind ausführbare MSI-Pakete und installieren neben TightGate®-Viewer auch das benötigte Programm zur Audioübertragung (Pulseaudio). Weiterhin ist eine Variante des TightGate®-Viewers verfügbar, die zugleich auch den TightGate®-Druckspooler installiert.

Bei der Installation der MSI-Pakete wird auf dem Desktop des Arbeitsplatz-PCs ein neues Icon angelegt, welches die Bezeichnung „Internet“ trägt. Durch einen Doppelklick auf das Icon wird TightGate®-Viewer gestartet.

6.2.2 Konfiguration

Konfiguration des TightGate®-Viewers für die Anmeldung mit Benutzername und Passwort

Es gibt zwei Arten von Konfigurationsdateien: eine systemweite und benutzerspezifische.

Die systemweite Konfigurationsdatei befindet sich unter

%PROGRAMFILES(X86)%\TightGate-Pro\tgpro.cfg

oder auf 32-Bit-Systemen unter

%PROGRAMFILES%\TightGate-Pro\tgpro.cfg

Die benutzerspezifischen Konfigurationsdatei ist im jeweiligen Benutzerkonto des Klientenrechners zu finden unter

%APPDATA%\vnc\tgpro.vnc

Wird TightGate®-Viewer ohne spezielle Parameter gestartet, dann liest dieser seine Konfiguration aus der benutzerspezifischen Konfigurationsdatei. Ist eine solche nicht vorhanden, dann liest TightGate®-Viewer die systemweite Konfigurationsdatei aus und legt bei Beendigung der Sitzung eine benutzerspezifische Konfigurationsdatei an. In dieser werden alle Änderungen gespeichert, die der User während einer Sitzung selbst vornimmt.

Nach der Installation des MSI-Pakets für TightGate®-Viewer sollte zunächst die systemweite Konfigurationsdatei ***tgpro.cfg*** angepasst werden, da diese von TightGate®-Viewer automatisch als Vorlage für alle Benutzerkonfigurationen auf dem jeweiligen Klientenrechner verwendet wird. Zwei Anpassungen sind zur Anmeldung mit Benutzername und Passwort notwendig:

1. Es muss die IPv4-Adresse oder der auflösbare Name von TightGate®-Pro Server in der Konfigurationsdatei ***tgpro.cfg*** hinter dem Eintrag „ServerName=“ oder hinter „host=“ eingetragen werden.
2. Außerdem muss hinter dem Eintrag „SecurityTypes=“ entweder „TLSPlain“ (Passwort-Anmeldung ohne Überprüfung des Serverzertifikates) oder „X509Plain“ (Passwort-Anmeldung mit Überprüfung des Serverzertifikates) eingefügt werden.

Hinweise:

- Zur Änderung der systemweiten Konfigurationsdatei ***tgpro.cfg*** sind Administratorrechte auf dem Zielsystem erforderlich.
- Nach dem ersten Start von TightGate®-Viewer wird für den jeweiligen Benutzer eine spezifische Konfigurationsdatei ***tgpro.vnc*** angelegt und fortan ausschließlich genutzt. Eventuelle spätere Änderungen an der systemweiten ***tgpro.cfg*** werden ignoriert. Sollen Änderungen vorgenommen werden, dann müssen diese an der benutzerspezifischen Datei geschehen. Alternativ kann die benutzerspezifische Datei gelöscht werden, dann wird beim nächsten Programmstart eine neue aus der systemweiten Datei erzeugt.
- Im Fall großer Nutzergruppen kann ein angepasstes MSI-Paket von der m-privacy GmbH bezogen werden, das die umgebungsspezifischen Einstellungen bereits berücksichtigt. Konfigurationsarbeiten an den Arbeitsplatzrechnern sind nach dem Rollout in diesem Fall nicht erforderlich.

Konfiguration des Viewers für das zertifikatsbasierte Single Sign-on

Für das zertifikatsbasierte Single Sign-on an TightGate®-Pro Server sollte sichergestellt sein, dass in der benutzerspezifischen oder (wenn diese nicht vorhanden ist) in der systemweiten Konfigurationsdatei hinter dem Eintrag „SecurityTypes=“ der Wert „X509Cert“ steht. Außerdem ist es erforderlich, dass die entsprechenden Zertifikate auf dem Arbeitsplatz-PC für jeden Benutzer in dessen Verzeichnis ***%APPDATA%\vnc*** hinterlegt sind.

Achtung: Firewalls und Paketfilter zwischen TightGate®-Pro Server und den Arbeitsplatzrechnern (Klientenrechner) müssen ebenso wie eventuell im Einsatz befindliche Desktop-Firewalls Datenverkehr von TightGate®-Pro Server zum Klienten auf den serverseitig konfigurierten Sound-Port 4713 zulassen. Andernfalls können keine Audiosignale übertragen werden. Wird keine Audioübertragung gewünscht, ist diese Option in der serverseitigen Konfiguration zu deaktivieren. Werden lediglich die Sound-Ports zur Übertragung der Tonsignale per Paketfilter blockiert, kommt es zu erheblichen Störungen bei der Videowiedergabe mit TightGate®-Pro.

Falls zwischen den Klienten und den TightGate®-Pro-Serversystemen eine Adressumsetzung (NAT) verwendet wird, kann die Klienten-IP-Adresse für die Audio-Verbindungen eventuell nicht korrekt ermittelt werden. Bitte wenden Sie sich in diesem Fall an die m-privacy GmbH.

6.2.3 Hinweise für Terminalserver-Anlagen (z. B. CITRIX)

Die Nutzung von TightGate®-Pro über Terminalserver-Anlagen ist möglich. Grundsätzlich erfolgt die Installation der Klientensoftware analog zur Vorgehensweise bei dedizierten Arbeitsplatzstationen. Es bestehen jedoch einige Besonderheiten im Hinblick auf die störungsfreie Bildschirmdarstellung sowie bei den notwendigen Portfreigaben für die Audioübertragung im internen Netzwerk.

Zunächst wird dringend empfohlen, die Option „Lokalen Mauszeiger statt Server-Mauszeiger verwenden“ in den Viewer-Programmen zu aktivieren, die in den Klientenkonten auf dem Terminalserver installiert werden. Dies kann auf unterschiedlichen Wegen geschehen.

Falls zur Authentisierung der Klienten am Server mit Single Sign-on (SSO) über die in TightGate®-Pro Server generierten Zertifikate gearbeitet wird, genügt es, vor der Erstellung der Zertifikate als Administrator ***config*** die Option ***config > Einstellungen > Authentisierung > Windows-Cursor in Klienten-Konfig.*** zu aktivieren. Hernach müssen die Zertifikate (bei Umstellung neu) erzeugt und verteilt werden. Die Viewer-Applikationen werden daraufhin automatisch so umgeschaltet, dass statt des Mauszeigers von TightGate®-Pro Server der Zeiger des Terminalservers angezeigt wird. Dies verhindert auf den Klientenrechnern Verzögerungen und Doppelbilder bei der Darstellung des Mauszeigers in Verbindung mit TightGate®-Pro.

Kommt Single Sign-on über die in TightGate®-Pro Server generierten Zertifikate nicht zum Einsatz, weil mit einem anderen Authentisierungsverfahren oder Zugangsdaten gearbeitet wird, muss die entsprechende Einstellung der Viewer-Programme TightGate®-Pro Client entweder manuell über deren Pro-

gramm-Menü (***F8 > Einstellungen …***, Registertaste „**Eingabemethode**“, Bereich „**Maus**“) oder per Konfigurationsdatei ***tgpro.vnc*** (Parameter **UseLocalCursor**, Datei zu finden in ***%APPDATA%/vnc***) vorgenommen werden. In bestimmten Fällen ist auch die Lieferung eines vorkonfigurierten Viewers als installationsfähiges MSI-Paket möglich. Der technische Kundendienst der m-privacy GmbH erteilt nähere Auskünfte.

Audiowiedergabe über Terminalserver-Klienten wird von TightGate®-Pro Server unterstützt. Hierfür müssen zwei Voraussetzungen erfüllt sein:

1. Konfiguration von TightGate®-Pro Server: Als Administrator ***config*** ist unter ***config > Einstellungen > Pulseaudio Extra-Ports*** ein zusätzlicher Portbereich auszuwählen, über den Audio-Signale übertragen werden sollen.
2. Konfiguration aktiver Netzwerkkomponenten: Alle Paketfilter und Firewalls, die zwischen TightGate®-Pro Server und Terminalserver respektive Terminalserver und Klienten geschaltet sind, müssen den Datenverkehr über die auf TightGate®-Pro Server konfigurierten, zusätzlichen Pulseaudio Extra-Ports passieren lassen.

Achtung: Die Konfiguration des Standard-Audioports 4713 auf TightGate®-Pro Server sowie dessen Freigabe in aktiven Netzwerkkomponenten ist zum Betrieb mit einem Terminalserver nicht ausreichend. Es kommt in diesem Fall keine Audiowiedergabe über TightGate®-Pro Server an den Klienten des Terminalservers zustande. Vom empfohlenen Zusatz-Portbereich sollte indessen nur in begründeten Ausnahmefällen abgewichen werden, da es sonst mitunter zu Störungen bei der Audiowiedergabe an direkt angebundenen Klientenrechnern kommen kann.

6.2.4 Hinweise zum Vollbildmodus / Umschaltung zwischen Applikationen

Mit der Tastenkombination ***ALT+Tab*** kann zwischen laufenden Applikationen umgeschaltet werden. Sofern der TightGate®-Viewer im Fenster-Modus betrieben wird, wirkt sich ***ALT+Tab*** nur auf die Umgebung außerhalb von TightGate®-Viewer aus. Im Vollbild-Modus wird hingegen zwischen laufenden Applikationen innerhalb des TightGate®-Viewers gewechselt.

Dieses Verhalten kann dahingehend geändert werden, dass auch im Vollbild-Modus ***ALT+Tab*** nicht an TightGate®-Pro Server weitergegeben wird. Die Tastenkombination wirkt sich dann in jedem Fall ausschließlich auf die Umgebung außerhalb von TightGate®-Viewer aus. Um dieses Verhalten zu konfigurieren, kann in der Konfigurationsdatei von TightGate®-Viewer der Parameter

FullScreenSystemKeys=0

gesetzt werden.

Alternativ kann im Fenstermenü des TightGate®-Viewers (Aufruf mit F8) unter

Einstellungen > Eingabemethoden > Systemtasten direkt zum Server senden

der Haken entfernt werden.

6.3 TightGate®-Viewer unter Apple OS X

Der TightGate®-Viewer steht derzeit ausschließlich für Apple OS X im Support-Bereich der Internetpräsenz der m-privacy GmbH lizenzkostenfrei zum Abruf bereit. Unterstützt wird OS X ab Version 10.9 (Mavericks). Das Betriebssystem iOS für mobile Endgeräte von Apple wird derzeit nicht unterstützt.

6.3.1 Installation

Das verfügbare DMG-Paket ist regulär ins Verzeichnissystem einzuhängen (Doppelklick). Der TightGate®-Viewer kann hernach in Programme-Verzeichnis verschoben werden (Benutzerauthentifizierung ist unter Umständen erforderlich). Grundsätzlich ist der TightGate®-Viewer für Apple OS X an jedem Speicherort lauffähig und umfasst sämtliche Komponenten wie beispielsweise auch Pulseaudio zur Wiedergabe von Audiodaten über TightGate®-Pro.

6.3.2 Konfiguration

Die Einrichtung des TightGate®-Viewers unter Apple OS X erfolgt entsprechend der Konfiguration unter Linux. Eine systemweite Konfigurationsdatei kann sich unter ***/etc/tgpro.cfg*** befinden, die benutzerspezifischen Dateien liegen unter ***~/.vnc/tgpro.vnc***. Die systemweite Konfigurationsdatei dient dabei als Template zur Generierung der benutzerspezifischen Datei, sofern diese nicht vorliegt. Die benutzerspezifische Datei wird nach jedem Beenden des TightGate®-Viewers mit den aktuellen Einstellungen des Viewers neu geschrieben. Wurden die Einstellungen des Viewers geändert, erfolgt die Sicherung der Änderungen in der benutzerspezifischen Konfigurationsdatei.

Die Konfigurationsdateien können im Terminalprogramm mittels eines Texteditors manuell angepasst werden. Hierzu ist es zunächst erforderlich, die Anzeige „versteckter“ Dateien (also solchen, die mit einem Punkt im Dateinamen beginnen), per Terminalbefehl einzuschalten:

```
defaults write com.apple.finder AppleShowAllFiles true
```

Nach Abschluss der Konfigurationsarbeiten können „versteckte“ Dateien wieder ausgeblendet werden mit dem Befehl

```
defaults write com.apple.finder AppleShowAllFiles false
```

In beiden Fällen muss der Finder (Dateimanager von Apple OS X) neu gestartet werden:

```
killall Finder
```

Konfiguration des Viewers für die Anmeldung mit Benutzername und Passwort

Wie unter Windows können vor dem ersten Programmstart in die systemweite oder in die benutzerspezifische Konfigurationsdatei die beiden Zeilen „ServerName=<IP-Adresse>“ und z. B. „SecurityTypes=TLSPlain“ (für Passwort-Login ohne Überprüfung des Serverzertifikates) eingetragen werden. Ist dies geschehen, dann genügt ein Aufruf des Programms via Programmicon, um die Verbindung zum TightGate®-Server herzustellen. Existiert noch keine der beiden Dateien, muss diese nicht unbedingt manuell mit einem Editor angelegt werden. Stattdessen löst der erstmalige Aufruf die Abfrage der IPv4-Adresse des Servers aus und initiiert die Verbindung mit Zugangsdaten. Wurde die IPv4-Adresse des Servers erstmalig eingegeben, legt TightGate®-Viewer automatisch ein Unterverzeichnis ***.vnc*** im Home-Verzeichnis des angemeldeten Benutzers an und erzeugt eine Konfigurationsdatei ***tgpro.vnc*** mit der IPv4-Adresse des Servers. Zur Verbindung mit demselben Server genügt fortan der Aufruf des TightGate®-Viewers, um unmittelbar zum Login-Dialog zu gelangen.

Konfiguration des Viewers für das zertifikatsbasierte Single Sign-on

Für das zertifikatsbasierte Single Sign-on an TightGate®-Pro Server sollte sichergestellt sein, dass in der benutzerspezifischen oder (wenn diese nicht vorhanden ist) in der systemweiten Konfigurationsdatei hinter dem Eintrag „SecurityTypes=“ der Wert „X509Cert“ steht. Außerdem ist es erforderlich, dass die entsprechenden Zertifikate auf dem Arbeitsplatz-PC für jeden Benutzer in dessen Verzeichnis ***~/.vnc*** hinterlegt sind.

Achtung: Firewalls und Paketfilter zwischen TightGate®-Pro Server und den Arbeitsplatzrechnern (Klientenrechner) müssen ebenso wie eventuell im Einsatz befindliche Desktop-Firewalls Datenverkehr von TightGate®-Pro Server zum Klienten auf den serverseitig konfigurierten Sound-Port 4713 zulassen. Andernfalls können keine Audiosignale übertragen werden. Wird keine Audioübertragung gewünscht, ist diese Option in der serverseitigen Konfiguration zu deaktivieren. Werden lediglich die Sound-Ports zur Übertragung der Tonsignale per Paketfilter blockiert, kommt es zu erheblichen Störungen bei der Videowiedergabe mit TightGate®-Pro.

6.4 TightGate®-Viewer unter Linux

Der TightGate®-Viewer steht für aktuelle Debian-basierte Distributionen im Support-Bereich der Internetpräsenz der m-privacy GmbH lizenzkostenfrei zum Abruf bereit.

6.4.1 Installation

Die bereitgestellten Pakete installieren nur den TightGate®-Viewer. Die für die Soundübertragung erforderlichen Programme sind distributionsspezifisch zusätzlich zu installieren. Benötigt werden alle Pakete für das Programm Pulseaudio, die weitergehende Konfiguration ist nicht erforderlich.

6.4.2 Konfiguration

Die Einrichtung des TightGate®-Viewers unter Linux erfolgt entsprechend der Konfiguration unter Windows. Lediglich die Konfigurationsdateien befinden sich an anderen Orten im Dateisystem. Eine systemweite Konfigurationsdatei kann sich unter ***/etc/tgpro.cfg*** befinden, die benutzerspezifischen Dateien liegen unter ***~/.vnc/tgpro.vnc***.

Konfiguration des Viewers für die Anmeldung mit Benutzername und Passwort

Wie unter Windows können vor dem ersten Programmstart in die systemweite oder in die benutzerspezifische Konfigurationsdatei die beiden Zeilen „ServerName=<IP-Adresse>“ und z. B. „SecurityTypes=TLSPlain“ (für Passwort-Login ohne Überprüfung des Serverzertifikates) eingetragen werden.

Ist dies geschehen, dann genügt ein Aufruf des Programms via

```
tightgateviewer
```

um die Verbindung zum TightGate®-Server herzustellen.

Existiert noch keine der beiden Dateien, muss diese nicht unbedingt manuell mit einem Editor angelegt werden. Stattdessen bewirkt der erstmalige Aufruf mittels

```
tightgateviewer <IP-Adresse des Servers>
```

eine Verbindung mit Zugangsdaten. Wurde die IPv4-Adresse des Servers erstmalig eingegeben, legt TightGate®-Viewer automatisch ein Unterverzeichnis ***.vnc*** im Home-Verzeichnis des angemeldeten Benutzers an und erzeugt eine Konfigurationsdatei ***tgpro.vnc*** mit der IPv4-Adresse des Servers. Zur Verbindung mit demselben Server genügt fortan die Eingabe von

```
tightgateviewer
```

um unmittelbar zum Login-Dialog zu gelangen. Alternativ kann der TightGate®-Viewer auch über das Startmenü gestartet werden.

Konfiguration des Viewers für das zertifikatsbasierte Single Sign-on
Für das zertifikatsbasierte Single Sign-on an TightGate®-Pro Server sollte sichergestellt sein, dass in der benutzerspezifischen oder (wenn diese nicht vorhanden ist) in der systemweiten Konfigurationsdatei hinter dem Eintrag „SecurityTypes=“ der Wert „X509Cert“ steht. Außerdem ist es erforderlich, dass die entsprechenden Zertifikate auf dem Arbeitsplatz-PC für jeden Benutzer in dessen Verzeichnis ***~/.vnc*** hinterlegt sind.

Achtung: Firewalls und Paketfilter zwischen TightGate®-Pro Server und den Arbeitsplatzrechnern (Klientenrechner) müssen ebenso wie eventuell im Einsatz befindliche Desktop-Firewalls Datenverkehr von TightGate®-Pro Server zum Klienten auf den serverseitig konfigurierten Sound-Port 4713 zulassen. Andernfalls können keine Audiosignale übertragen werden. Wird keine Audioübertragung gewünscht, ist diese Option in der serverseitigen Konfiguration zu deaktivieren. Werden lediglich die Sound-Ports zur Übertragung der Tonsignale per Paketfilter blockiert, kommt es zu erheblichen Störungen bei der Videowiedergabe mit TightGate®-Pro.

6.5 Schleusenprogramm unter Microsoft® Windows®

6.5.1 Installation

Die über den Support-Bereich der Internetpräsenz der m-privacy GmbH bereitgestellten, ausführbaren MSI-Pakete installieren die TightGate®-Schleuse. Bei der Installation der MSI-Pakete wird auf dem Desktop des Arbeitsplatz-PCs ein neues Icon angelegt, welches die Bezeichnung „Schleuse“ trägt. Durch einen Doppelklick auf das Icon wird die TightGate®-Schleuse gestartet.

Hinweis: Alle Varianten der TightGate®-Schleuse ermöglichen eine weitreichende Konfiguration der Bildschirmansicht. Damit kann die Darstellung des Schleusenfensters sowie der Dateieinträge den Bedürfnissen der Anwender angepasst werden. Standardmäßig startet TightGate®-Schleuse in der deutlich funktionsreicheren „Commander“-Ansicht, kann jedoch auf die „Explorer“-Ansicht mit weniger Bedienelementen umgeschaltet werden. Beide Bildschirmansichten sind konfigurierbar. Nähere Auskünfte hierzu erteilt der technische Kundendienst der m-privacy GmbH.

Die Einstelloptionen unterscheiden sich je nach verwendetem Betriebssystem und sind über die Fenstermenüs respektive Programmmenüs der Schleusenprogramme zugänglich. Sie werden im folgenden nicht eingehender beschrieben. Nähere Auskünfte erteilt der technische Kundendienst der m-privacy GmbH, über den auch angepasste Konfigurationsdateien zum Roll-out in größeren Infrastrukturen erhältlich sind.

In der Grundkonfiguration startet die TightGate®-Schleuse nach Installation betriebsbereit mit allen verfügbaren Auswahloptionen und Bedienelementen.

6.5.2 Konfiguration

**Konfiguration der Dateischleuse unter Microsoft® Windows®
für die Anmeldung mit Zugangsdaten (Benutzername und Passwort)**

Achtung: Die Schleuse kann nur benutzt werden, wenn die Schleusennutzung durch den Administrator ***config*** systemweit zugelassen ist und der Administrator ***maint*** die benutzerindividuelle Berechtigung zur Schleusennutzung erteilt hat.

Nach der Installation des MSI-Pakets für die Dateischleuse von TightGate®-Pro muss die IPv4-Adresse oder der auflösbare DNS-Name von TightGate®-Pro in der Konfigurationsdatei **transfer.ini** hinter dem Eintrag „IP-Adresse von TightGate®-Pro“ eingetragen werden.

Die Konfigurationsdatei **transfer.ini** befindet sich unter Microsoft® Windows® in

%APPDATA%\vnc

Es empfiehlt sich, eine Kopie der Datei zu editieren. Abschließend ist die Datei ***transfer.ini*** wieder an ihren bisherigen Ort zu speichern.

Hinweise:

- Im Fall großer Nutzergruppen kann ein angepasstes MSI-Paket von der m-privacy GmbH bezogen werden, das die umgebungsspezifischen Einstellungen bereits enthält.
- Die Anmeldung erfolgt mit den gleichen Zugangsdaten, wie sie für die Anmeldung an TightGate®-Pro Server verwendet werden.

Konfiguration der Dateischleuse für das zertifikatsbasierte Single Sign-on
Eine Konfiguration der Dateischleuse für das zertifikatsbasierte Single Sign-on an TightGate®-Pro Server ist nicht notwendig. Es ist jedoch vor der ersten Anmeldung sicherzustellen, dass die entsprechenden Zertifikate und die vom Server generierte ***transfer.ini*** auf dem Arbeitsplatz-PC im Verzeichnis ***%APPDATA%\vnc*** hinterlegt sind.

Hinweis: Die Nutzung der Dateischleuse mit zertifikatsbasiertem Single Sign-on erfordert zwingend eine vorangehende, einmalige Anmeldung über den Viewer an TightGate®-Pro Server. In allen folgenden Sitzungen kann die Schleuse wahlweise auch vor dem Viewer oder exklusiv gestartet werden. Bei

Clustersystemen ist die Nutzung der Dateischleuse nach einer Wartezeit bis zu 10 Minuten nach der erstmaligen Anmeldung über den Viewer an TightGate®-Pro Server möglich. Die Wartezeit entfällt bei allem folgenden Anmeldevorgängen, solange das verwendete Zertifikat dasselbe bleibt.

Konfiguration der Dateischleuse für das KERBEROS-basierte Single Sign-on (Active Directory)
Die Schleuse kann die notwendige Konfigurationsdatei

%APPDATA%\vnc\transfer.ini

selbst erzeugen, sofern in der systemweiten Konfigurationsdatei

%PROGRAMFILES(X86)%\TightGate-Pro\tgpro.cfg

die Werte „ServerName“ und „KrbHostName“ gesetzt sind, und der Eintrag „SecurityTypes“ den Wert „X509Krb“ enthält.

6.6 Schleusenprogramm unter Apple OS X

Für die Benutzung der Dateischleuse unter Apple OS X eignet sich ein beliebiges Programm zur Dateiübertragung nach dem SFTP-Protokoll. Insbesondere das Programm ***Cyberduck*** hat sich zum Datenaustausch zwischen TightGate®-Pro Server und einem Apple-Arbeitsplatzrechner bewährt. Damit lässt sich auch eine zertifikatsbasierte Anmeldung einrichten. Näheres entnehmen Sie bitte der Dokumentation zum Programm oder konsultieren Sie den technischen Kundendienst der m-privacy GmbH.

6.6.1 Installation

Die Installation erfolgt nach Abruf und entpacken des Archivs unter Apple OS X durch einfaches Verschieben der Applikation in das Programmverzeichnis. ***Cyberduck*** ist unmittelbar lauffähig. Ein Installer muss nicht durchaufen werden.

Achtung: Die Applikation sollte ausschließlich von der Internetpräsenz der Entwickler heruntergeladen werden.

6.6.2 Konfiguration

Die Konfiguration erfolgt mit den üblichen Parametern analog zur Konfiguration unter Linux. Bei Bedarf sollte die Dokumentation des Programms zurate gezogen werden. Der technische Kundendienst der m-privacy GmbH leistet auf Anfrage Unterstützung bei der Konfiguration; hierfür können gesonderte Kosten anfallen.

6.7 Schleusenprogramm unter Linux

6.7.1 Installation

Für die Benutzung der Dateischleuse unter Linux eignet sich ein beliebiges Programm zur Dateiübertragung nach dem SFTP-Protokoll. Insbesondere das Programm **gftp** hat sich zum Datenaustausch zwischen TightGate®-Pro Server und einem Arbeitsplatzrechner bewährt. Es gehört zum Standardumfang der meisten Distributionen, muss jedoch üblicherweise über die Paketverwaltung nachinstalliert werden.

6.7.2 Konfiguration

Beispiel: Konfiguration von gftp für die Anmeldung mit Benutzername und Passwort

- Angabe des Rechners: IPv4-Adresse oder auflösbarer Hostnamen von TightGate®-Pro Server
- Port: nicht erforderlich
- Nutzername: Benutzername auf TightGate®-Pro Server
- Passwort: Passwort auf TightGate®-Pro Server
- Protokoll: SSH2

Die Verbindung wird nach Klick auf das Verbindungs-Icon hergestellt.

Konfiguration der Dateischleuse für das zertifikatsbasierte Single Sign-on
Die Unterstützung für Single Sign-on unter Linux ist derzeit mit dem SFTP-Klienten „Filezilla“ möglich. Es kann lizenzkostenfrei bezogen werden. Nähere Informationen erteilt der technische Kundendienst der m-privacy GmbH.

6.8 Teilautomatische Browserweiche “MagicURL“

Das Viewer-Programm (TightGate®-Pro Client) kann mit der teilautomatischen Browserweiche MagicURL kombiniert werden. Nach Installation und Konfiguration werden Internetadressen (URLs) aus lokal installierten Drittapplikationen automatisch wahlweise im lokalen Browser oder über TightGate®-Pro angezeigt werden.

MagicURL kann als installierbares Programmpaket (MSI-Paket) über den Supportbereich der Internetpräsenz der m-privacy GmbH bezogen werden. Die notwendige Konfiguration der umzuleitenden URLs kann anwenderseitig vorgenommen werden. Sie kann auch zentral erstellt und auf die Klientenrechner verteilt werden.

6.8.1 Arbeitsweise

MagicURL arbeitet nur auf Klientenrechnern, die mit den Betriebssystemen Microsoft® Windows® 7 32/64Bit oder Microsoft® Windows® Server 2008 versehen sind. Es implementiert eine halbautomatische Browserweiche, wobei alle Internetadressen (URLs), die sich in einer Positivliste (WhiteList) befinden, an den lokal installierten Webbrowser übergeben werden. Alle anderen URLs werden automatisch im Browser von TightGate®-Pro geöffnet. MagicURL klinkt sich dabei anstelle des Standard-Browsers im Betriebssystem ein, sodass alle URLs aus externen Programmen geprüft und entsprechend verarbeitet werden können.

6.8.2 Einschränkungen

MagicURL kann nur Internetadressen (Links, URLs) auf dem Klientenrechner verarbeiten, die nicht unmittelbar aus einem Internetbrowser stammen. Adressen aus E-Mail-Programmen oder Anwendersoftware wie beispielsweise Textverarbeitungsprogrammen oder anderen Office-Applikationen können durch MagicURL dem entsprechenden Browser automatisiert zugeleitet werden. Bei URLs, die bereits über TightGate®-Pro angezeigt werden, erfolgt auch der Aufruf immer über TightGate®-Pro. Externe URLs, die im lokalen Browser angezeigt werden, werden über den lokalen Browser aufgerufen – was fehlschlägt, da dieser in Infrastrukturen mit TightGate®-Pro im Regelfall keine externen Internetverbindungen aufbauen darf.

Hinweis: URLs, die unter TightGate®-Pro angezeigt werden, jedoch nur intern zu öffnen sind, müssen mittels Kopieren und Einfügen (Copy & Paste) in den lokalen Browser transferiert werden. Gleiches gilt für URLs, die im lokalen Browser angezeigt werden, jedoch auf externe Ressourcen zugreifen (etwa bei der Nutzung eines Unternehmens-Intranets). In diesem Fall ist die jeweilige Adresse über die Zwischenablage nach TightGate®-Pro zu übertragen und im dortigen Browser einzufügen.

6.8.3 Installation

Zur Installation von MagicURL ist ein MSI-Paket aus dem Support-Bereich der Internetpräsenz der m-privacy GmbH abzurufen und auf den Klientenrechnern zu installieren. Parallel zur Installation des MagicURL-Pakets sind folgende Einstellungen als Administrator ***config*** auf TightGate®-Pro vorzunehmen:

1. Unter ***Einstellungen > Magische URLs*** ist die Verwendung zu aktivieren.
2. Unter ***Einstellungen > Zwischenablage*** ist entweder der Wert ***Klient zu Server*** oder ***Vollduplex*** auszuwählen.

Das MSI-Paket legt die benötigte Programmdatei im Installationsverzeichnis von TightGate®-Pro an.

6.8.4 URL-Positivliste (WhiteList)

Die URL-Whitelist ist eine einfache Textdatei und dient zur Festlegung von Internetadressen (URLs), die im lokalen Browser angezeigt werden sollen. Die Daten werden unter ***%APPDATA%\vnc*** in der Datei ***url_whitelist.txt*** gespeichert. Diese Datei kann seitens der Systemadministration erzeugt und verteilt werden, um größeren Benutzergruppen die Anzeige lokaler Ressourcen im lokalen Browser ohne weitere Konfiguration zu ermöglichen. Beim ersten Aufruf einer URL, welche über MagicURL verarbeitet wird legt das System die Datei ***url_whitelist.txt*** an, sofern diese noch nicht existiert.

6.8.5 Konfiguration lokaler Internetadressen (URLs)

Die Festlegung der lokalen URLs in der Positivliste kann über einen beliebigen Texteditor erfolgen. Folgendes ist bei der Bearbeitung der URL-Whitelist zu beachten:

- Die Domain-Whitelist-Datei ist eine normale Textdatei.
- Pro Zeile ist nur eine Domain einzutragen und die Zeile darf keine Leerzeichen enthalten.
- Es gibt keine Beschränkung bei der Anzahl der definierbaren Domains/URLs.
- Alle mit einem # versehenen Zeilen und Leerzeilen werden nicht ausgewertet.
- Das *-Zeichen dient als Platzhalter für beliebigen Text.

Folgende Syntax ist bei der Eingabe interner Adressen über den Editor zulässig:

Beispiel	Hinweise
.m-privacy.de/	MagicURL erkennt in diesem Fall alle Anfragen, welche .m-privacy.de/ enthalten. Das Wildcard * als Platzhalter beinhaltet dabei die Angaben von „www“. Das * hinter der Domain schließt alle nachfolgenden Unterseiten ein. Folgende Seiten würde das Beispiel beinhalten: • m-privacy.de • www.m-privacy.de • blog.m-privacy.de/meldungen • http://m-privacy.de • https://www.m-privacy.de/support/download-center/index.html
192.168.34.*	MagicURL erkennt alle Anfragen zu dem IP-Adressbereich 192.168.34.X als lokale Adressen und leitet sie dem lokal installierten Browser zu. Es erfolgt jedoch keine Namensauflösung. Die Angabe von http:// oder https:// ist nicht notwendig, MagicURL erkennt diese Angaben automatisch.

Hinweis: Bei der Übernahme von URLs aus einen PDF-Dokument gibt es ein Fehlverhalten beim Adobe Reader der Versionen 9 und 10. Hierbei werden alle URL-Aufrufe nur an den lokalen Internet Explorer übergeben, sobald dieser läuft. Den Fehler hat Adobe in der Adobe Reader Version ab Version 11 behoben. Sofern Sie von diesem Problem betroffen sind, aktualisieren Sie bitte den Adobe Reader.

7 Nutzung von TightGate®-Pro mit Active Directory

Neben der in TightGate®-Pro Server integrierten Benutzerverwaltung ist auch die zentrale Administration über ein vorhandenes Active Directory (AD) möglich. Wird TightGate®-Pro Server an diesen Verzeichnisdienst angebunden, können Benutzer automatisch per Single Sign-on authentisiert werden, sobald sie sich an ihrer Arbeitsplatzstation in derselben AD-Domäne angemeldet haben. Weiterhin können wesentliche Merkmale der Benutzerkonten zentral im AD gepflegt werden, was die Verwaltung von TightGate®-Pro Server speziell in größeren Infrastrukturen signifikant erleichtert.

7.1 Voraussetzungen und Procedere

Zur Anbindung von TightGate®-Pro Server an ein Active Directory sind bestimmte Voraussetzungen zu erfüllen. Anschließend empfiehlt es sich, die einzelnen Schritte der nachfolgenden Anleitung nachzuvollziehen, um eine problemlose Inbetriebnahme zu gewährleisten. Im ersten Schritt sind die Systemvoraussetzungen sicherzustellen, dann erfolgt die Konfiguration des AD-Servers und abschließend die Konfiguration von TightGate®-Pro Server.

Die notwendigen Schritte unterscheiden sich je nach dem, ob ein Einzelsystem oder ein Rechnerverbund (Clustersystem) von TightGate®-Pro Server an ein Active Directory angebunden werden soll. Es ist darauf zu achten, die richtigen Einstellungen für den jeweiligen Anwendungsfall vorzunehmen. Im Fall von Fehlfunktionen empfiehlt sich zunächst die erneute Kontrolle, ob alle Konfigurationsschritte vollständig und korrekt vorgenommen wurden.

Hinweis: Bei persistierenden Problemen im Zuge der Einstellarbeiten sollte der technische Kundendienst der m-privacy GmbH konsultiert werden.

7.1.1 Systemvoraussetzungen

TightGate®-Pro Server muss in jedem Fall auf aktuellem Softwarestand sein, da es andernfalls im Zuge der Anbindung an ein Active Directory zu Fehlern kommen kann. Weiterhin ist ein betriebsbereiter Microsoft® Windows® Server 2008R2 erforderlich, dieser muss sich ebenfalls auf aktuellem Softwarestand befinden.

Hinweis: Eine Unterstützung vom Windows® Server 2012 ist derzeit in Vorbereitung.

Nachfolgende Aufstellung fasst die benötigten Angaben im Vorfeld einer Einrichtung des Active Directory zur Verwendung mit TightGate®-Pro Server zusammen. Die verwendeten Beispielwerte dienen nur der Veranschaulichung, sie sind durch die korrekten Werte im jeweiligen Anwendungskontext zu ersetzen.

Achtung: Es bestehen wichtige Unterschiede hinsichtlich der grundlegenden Parameter zwischen der Einrichtung eines Einzelsystems und eines Clustersystems (Rechnerverbund) von TightGate®-Pro Server.

a) Parameterübersicht zur Anbindung eines Einzelsystems TightGate®-Pro Server

Bezeichnung	Beschreibung	Beispielwert
ADS-REALM	Domäne des AD-Servers. **Achtung:** Schreibung in Großbuchstaben ist obligatorisch.	SSO.M-PRIVACY.HOM
IPv4 AD-Server	IPv4-Adresse des Servers, auf dem das AD gehostet wird.	192.168.4.208
DNS-Name AD-Server	Auflösbarer Name des AD-Servers.	win2008
DNS	IPv4-Adresse des AD-Servers, der zugleich als DNS fungiert.	192.168.4.208
Domäne TG-Pro	Domäne, in der sich TightGate®-Pro Server befindet. Bei Einzelsystemen identisch mit dem ADS-REALM. **Achtung:** Schreibung in Kleinbuchstaben ist obligatorisch!	sso.m-privacy.hom
IPv4 NTP	IPv4-Adresse eines NTP-Zeitservers	192.168.4.254
IPv4 TG-Pro	IPv4-Adresse des TightGate®-Pro Server, auf dem sich Benutzer anmelden.	192.168.4.202
DNS-Name TG-Pro	Auflösbarer Name des TightGate®-Pro Server, auf dem sich die authentisierten Benutzer anmelden. Entspricht dem Computer-Account auf dem ADS.	TGPro

b Parameterübersicht zur Anbindung eines Clustersystems TightGate®-Pro Server

Bezeichnung	Beschreibung	Beispielwert
ADS-REALM	Domäne des AD-Servers. **Achtung:** Schreibung in Großbuchstaben ist obligatorisch.	SSO.M-PRIVACY.HOM
IPv4 AD-Server	IPv4-Adresse des Servers, auf dem das AD gehostet wird.	192.168.4.208
DNS-Name AD-Server	Auflösbarer Name des AD-Servers.	win2008
DNS	IPv4-Adresse des AD-Servers, der zugleich als DNS fungiert.	192.168.4.208
Domäne TG-Pro	Domäne, in der sich TightGate®-Pro Server befindet. Bei Einzelsystemen identisch mit dem ADS-REALM. Auflösbarer Name des TightGate®-Pro Clusters, auf dem sich die authentisierten Benutzer anmelden. **Achtung:** Schreibung in Kleinbuchstaben ist obligatorisch!	cluster.internet.netz
IPv4 NTP	IPv4-Adresse eines NTP-Zeitservers	192.168.4.254
IPv4 TG-Pro	IPv4-Adressen der TightGate®-Pro Server, auf dem sich Benutzer anmelden. Im Beispiel handelt es sich um einen Cluster aus 4 Rechnern (Nodes)	192.168.7.201 bis 192.168.7.204
Loadbalancer auf TG-Pro	Die für die Lastverteilung zuständigen Nodes des TightGate®-Pro Clusters	192.168.7.201 und 192.168.7.202
Computer-Name von TG-Pro im AD	Computer-Account auf dem ADS.	srv-TGPro

7.1.2 Klientenseitige Installation

Das Zusammenwirken von TightGate®-Pro Server mit einem Active Directory ist ausschließlich mit den hierzu vorgesehenen Viewer-Programmen (TightGate®-Viewer) möglich. Diese sind im Download-Bereich der m-privacy GmbH verfügbar und können lizenzkostenfrei auf beliebig vielen Klientenrechnern installiert werden. Gleiches gilt entsprechend für das Schleusenprogramm TightGate®-Schleuse zur Nutzung der gesicherten Dateischleuse von TightGate®-Pro Server.

Achtung: Ohne Installation der dedizierten Viewer- und Schleusen-Applikationen ist eine Authentisierung gegen ein Active Directory nicht möglich. Die verfügbaren TightGate®-Viewer unterstützen Microsoft® Windows® 7 und 8 (32/64-Bit-Versionen). Windows® XP wird im Zusammenhang mit einer Anbindung von TightGate®-Pro Server an ein Active Directory von den verfügbaren Viewer-Applikationen **nicht** unterstützt. Der Viewer unter Linux unterstützt Active Directory, sofern bei seinem Start die notwendigen Kerberos-Tickets im System vorhanden sind.

Nach der Installation der Viewer-Applikation TightGate®-Viewer ist die Konfigurationsdatei ***tgpro.vnc*** (oder die systemweite Konfigurationsdatei ***tgpro.cfg***) mittels eines Texteditors manuell anzupassen, falls nicht herstellerseitig geschehen und bereits im Installationspaket des Viewers berücksichtigt. Hierzu ist bei den Parametern ***ServerName*** oder ***Host*** (diese Bezeichnungen sind gleichbedeutend) und ***KrbHostName*** der auflösbare Name des Einzelsystems oder des Clustersystems (Verbundrechners) TightGate®-Pro Server zu setzen, zu dem sich die Benutzer verbinden. Dieses Vorgehen entspricht der üblichen Verfahrensweise nach Installation des Viewers für andere Authentisierungsarten.

Des Weiteren muss zur Nutzung von Active Directory in der Konfigurationsdatei der Parameter „SecurityTypes“ auf „X509Krb“ gesetzt werden.

Es ist zu beachten, dass zum TightGate®-Viewer nur die passende Konfigurationsdatei ***tgpro.vnc*** (oder ***tgpro.cfg***) in gleicher oder älterer Version verwendet werden darf. Wird auf eine ältere Version des TightGate®-Viewers zurückmigriert, ist auch die ältere Version der Konfigurationsdatei neu aufzuspielen. Einer neuerer Viewer kann jedoch selbständig eine veraltete Konfigurationsdatei übernehmen und anpassen.

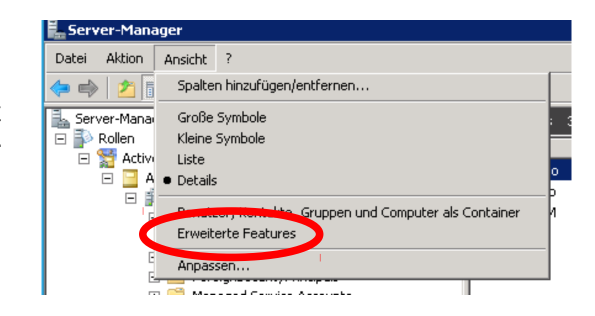
Sind die Active Directory-Einstellungen in der systemweiten Viewer-Konfigurationsdatei tgpro.cfg richtig gesetzt, dann kann auch die Schleuse bei ihrem Start ihre eigene Konfigurationsdatei %APPDATA%\vnc\transfer.ini automatisch erzeugen. Dies tut sie jedoch nur, wenn noch keine transfer.ini vorhanden ist.

Achtung: Bei Verbundrechnersystemen dürfen an dieser Stelle nicht die einzelnen Nodes referenziert werden!

7.1.3 Grundeinstellung von Windows® Server 2008 R2

Windows® Server 2008 R2 ist vor der Einrichtung der Anbindung eines TightGate®-Pro Server grundsätzlich zur Verarbeitung von Domänendiensten vorzubereiten, falls noch nicht geschehen.

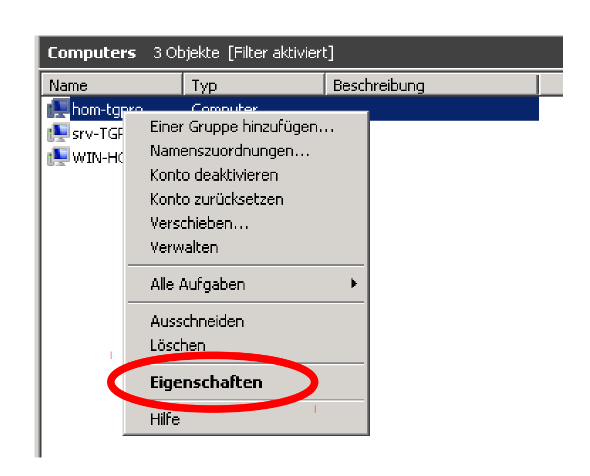
7.2 Konfiguration des AD-Servers

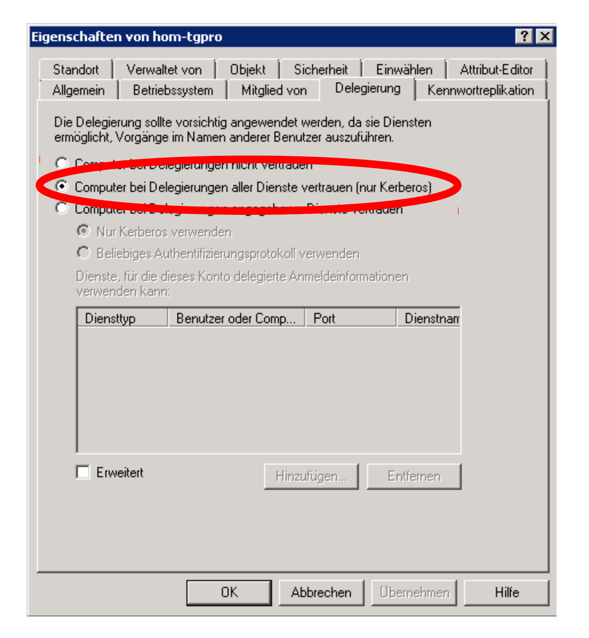


Zunächst ist TightGate®-Pro Server auf dem AD-Server als sogenannter Computer-Account anzulegen. Dies gilt für Einzelsysteme wie auch für Rechnerverbünde (Clustersysteme) gleichermaßen. Im Beispiel heißt der Computer-Account auf dem AD-Server im Fall eines Einzelsystems **TGPro** und im Fall eines Clustersystems **srv-TGPro**. Anschließend ist dieser Computer-Account weiter anzupassen. Im Server-Manager kann hierzu unter ***Ansicht > Erweiterte Features*** eine ausführlichere Liste der einzelnen Bestandteile der Domäne des AD-Servers (ADS-REALM) angezeigt werden.

7.2.1 Delegierung und Verschlüsselung

Die Liste der vorhandenen Computer-Accounts wird nach Klick mit der linken Maustaste auf ***Computers*** angezeigt.



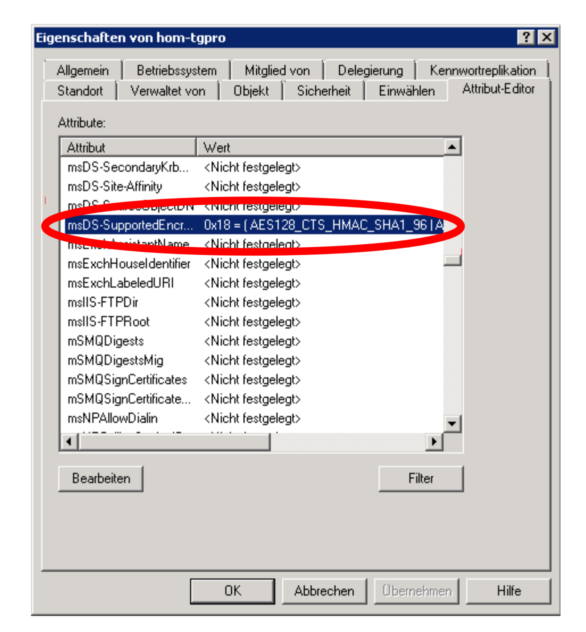


Ein Klick mit der rechten Maustaste auf den Computer-Account von TightGate®-Pro Server, im Beispiel entweder ***TGPro*** oder **srv-TGPro**, öffnet ein Kontextmenü, aus dem der Konfigurationsdialog über ***Eigenschaften*** aufzurufen ist.

Auf der Registertaste ***Delegierung*** ist die zweite Option ***Computer bei Delegierungen aller Dienste vertrauen (nur Kerberos)*** auszuwählen.

Im nächsten Schritt müssen Einstellungen im Attribut-Editor vorgenommen werden.

Sowohl für Einzel- als auch für Clustersysteme sind auf der Registertaste ***Attribut-Editor*** die Verschlüsselungstypen für den Computer-Account von TightGate®-Pro Server zu setzen. Dabei ist ausschließlich der Wert ***msDS-SupportedEncryption Types*** aus der Auswahlliste auf den Dezimalwert 24 (hexadezimal 0x18) zu setzen. Hierzu wird der betreffende Parameter in der Auswahlliste durch Klick mit der linken Maustaste selektiert (farbige Unterlegung sichtbar) und mittels Klick auf die Schaltfläche ***Bearbeiten*** zur Änderung freigeschaltet.



Nur für Clustersysteme muss weiterhin das Attribut servicePrincipalName auf den Wert ***host/[Domäne des TG-Pro-Clusters]*** gesetzt werden. Der Eintrag lautet demzufolge im Beispiel: ***host/cluster.internet.netz***.

7.2.2 Eintrag im DNS-Server für Einzelsysteme

Anschließend muss der Menübaum unter ***DNS-Server*** so weit ausgeklappt werden, bis die verfügbaren ***Forward-Lookupzonen*** sichtbar sind. Nach Klick mit der rechten Maustaste auf der entsprechenden Domäne des AD-Servers (ADS-REALM), in diesem Beispiel SSO.M-PRIVACY.HOM, kann über ***Neuer Host (A oder AAAA) …*** ein Dialog aufgerufen werden, über den der konkrete TightGate®-Pro Server zugewiesen werden kann.

Als Name ist der auflösbare Name von TightGate®-Pro Server anzugeben, ebenso wie die IPv4-Adresse des Servers. Das Kontrollkästchen ***Verknüpften PTR-Eintrag erstellen*** ist in jedem Fall zu aktivieren, damit der Hostname automatisch auch in der Reverse-Lookup-Zone eingetragen wird. Das Dialogfeld ist über die Schaltfläche ***Host hinzufügen*** zu verlassen. Es empfiehlt sich eine Überprüfung, ob der Name von TightGate®-Pro Server vorwärts und rückwärts korrekt aufgelöst werden kann.

7.2.3 Eintrag im DNS-Server für Clustersysteme

Leistungsstarke ReCoB-Server der TightGate®-Pro-Produktlinie werden aus Kapazitätsgründen stets als Rechnerverbund (Cluster) ausgeführt. Dieser Rechnerverbund besteht aus mehreren Einzelrechnern, die „Nodes“ genannt werden. TightGate®-Pro Server verfügt über eine automatische Lastverteilung. Diese Lastverteilung, auch „Load Balancing“ genannt, ist die Grundlage eines optimierten Systembetriebs. Je nach aktueller Beanspruchung der einzelnen Nodes werden neue Verbindungsanfragen an den jeweils am wenigsten belasteten Rechner des Verbunds übergeben.

In jedem TightGate®-Pro-Server-Cluster sind in Abhängigkeit von der Gesamtzahl der Einzelrechner mehrere der Nodes zusätzlich zu ihren eigentlichen Aufgaben als Load Balancer im Einsatz. Sie prüfen in kurzen Abständen die Belastungssituation im Rechnerverbund und entscheiden bei einer Verbindungsanfrage, welcher Node die neue Benutzersitzung übernehmen wird.

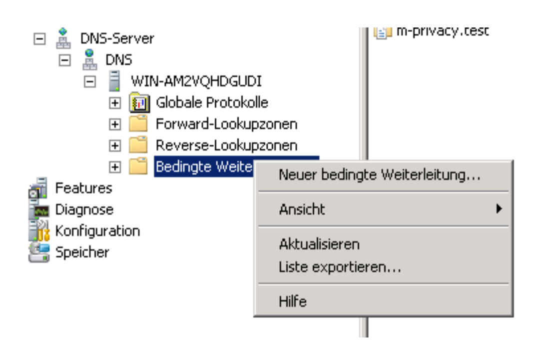
Damit die Lastverteilung einwandfrei arbeitet, dürfen die einzelnen Rechner im Verbund seitens der Klientenrechner nicht dediziert über deren IPv4-Adresse angesprochen werden. Stattdessen muss der gesamte Cluster von TightGate®-Pro Server im internen Netzwerk als Einheit erscheinen. Zusätzlich sind alle neuen Verbindungsanfragen zunächst an die Nodes zu übermitteln, welche die Aufgabe der Lastverteilung wahrnehmen.

Dies wird erreicht, indem die Verbindungsanfragen an einen zentralen Rechnernamen gestellt werden, der den Rechnerverbund repräsentiert. Die separate DNS-Zone für den Cluster nimmt die einzelnen Nodes des ReCoB-Systems aus der Verwaltung des lokalen DNS-Servers aus. Stattdessen übernimmt die Lastverteilung von TightGate®-Pro Server die interne Adresskoordination des Rechnerverbunds entsprechend der aktuellen Lastsituation.

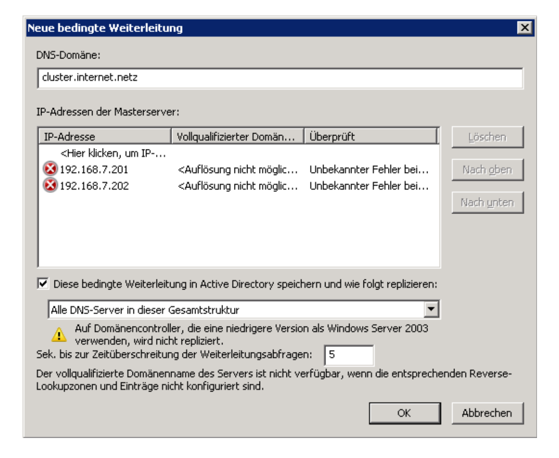
Die nachfolgende Anleitung beschreibt die Einrichtung einer DNS-Zonenweiterleitung (DNS Zone Forwarding) unter Microsoft® Windows® Server 2008R2.

a) Einstellungen am DNS-Server (win 2008)

1. Auswahl des Menüpunkts
   Bedingte Weiterleitung >
   Neue bedingte Weiterleitung...



2. In dem sich öffnenden Dialogfenster ist unter „DNS-Domäne“ der Domänenname des TightGate®-Pro Clusters (im Beispiel: cluster.internet.netz) einzutragen. Zusätzlich sind die IPv4-Adressen der Load Balancer des TightGate®-Pro-Clusters als „IP-Adressen der Masterserver“ hinzuzufügen. Im Beispiel werden die IPv4-Adressen der Nodes 192.168.7.201 und 192.168.7.202 hinzugefügt, da diese in diesem Fall als Load Balancer fungieren.



3. Als Nächstes ist in den Kasten neben den „Sek. bis zur Zeitüberschreitung der Weiterleitungs-abfragen" eine ***2*** zu setzen.
4. Abschließend die Einstellungen das Dialogfeld mit ***OK*** verlassen.

b) Rückwärtsauflösung einrichten (Reverse Lookupzone)

1. Auswahl des Menüpunkts ***Reverse Lookupzonen > Neue Zone...***
2. Dem Assistenten zur Erstellung einer Reverse Lookupzone für die Domäne des Clusters von TightGate®-Pro Server (im Beispiel cluster.internet.netz) folgen.

7.2.4 Definition der AD-Sicherheitsgruppen

Damit die Gruppenverwaltung von TightGate®-Pro Server korrekt auf das Active Directory übertragen wird, müssen die entsprechenden Sicherheitsgruppen auf dem zentralen Verzeichnisdienst angelegt sein. Es ist nicht notwendig, diese Sicherheitsgruppen manuell zu erstellen. Stattdessen genügt es, eine generische Konfigurationsdatei, eine sogenannte ldiff-Datei abzurufen, diese für die jeweilige Anwendungsumgebung anzupassen und die modifizierte Konfigurationsdatei nachfolgend in den AD-Server einzulesen.

Eine bereits angepasste ldiff-Datei kann im Download-Bereich der m-privacy-Internetpräsenz unter http://www.m-privacy.de/support/download-center/ abgerufen werden.

Hinweis: Nach dem entpacken sollte per Suchen_&_Ersetzen in einem Editor der String "DC=SSO,DC=M-PRIVACY,DC=HOM" mit dem jeweils eigenen Werten ersetzt werden! Die angepasste Datei tgpro.ldf kann anschließend unter Windows® über die Windows-PowerShell eingelesen werden.

Die ldiff-Datei hat einen regelmäßigen Aufbau und bildet die Gruppenstruktur von TightGate®-Pro Server auf die Sicherheitsgruppen des AD-Servers ab. Sie ist nachfolgend abgebildet und für jede Gruppe in der Zeile (CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM) anzupassen. Es sind die jeweiligen Bestandteile der Domäne des AD-Servers (ADS-REALM) einzutragen:

```
dn: CN=TGProUser,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGProUser
description: TightGate-Pro Nutzungsberechtigung
sAMAccountName: TGProUser

dn: CN=TGaudio,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGaudio
description: TightGate-Pro Berechtigung Audio
sAMAccountName: TGaudio

dn: CN=TGadminMaint,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGadminMaint
description: TightGate-Pro Administrator Maint
sAMAccountName: TGadminMaint

dn: CN=TGadminConfig,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGadminConfig
description: TightGate-Pro Administrator Config
sAMAccountName: TGadminConfig
```

```
dn: CN=TGadminUpdate,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGadminUpdate
description: TightGate-Pro Administrator Update
sAMAccountName: TGadminUpdate

dn: CN=TGadminBackuser,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGadminBackuser
description: TightGate-Pro Administrator Backup
sAMAccountName: TGadminBackuser

dn: CN=TGadminRoot,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGadminRoot
description: TightGate-Pro Administrator Root
sAMAccountName: TGadminRoot

dn: CN=TGadminSecurity,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGadminSecurity
description: TightGate-Pro Administrator Security
sAMAccountName: TGadminSecurity

dn: CN=TGprivileged,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGprivileged
description: TightGate-Pro Privilegierter Nutzer
sAMAccountName: TGprivileged

dn: CN=TGunfiltered,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGunfiltered
description: TightGate-Pro Ungefiltertes Web
sAMAccountName: TGunfiltered

dn: CN=TGtransferSpool,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGtransferSpool
description: TightGate-Pro Windows-Drucken
sAMAccountName: TGtransferSpool
dn: CN=TGtransfer,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGtransfer
description: TightGate-Pro Dateischleuse
sAMAccountName: TGtransfer
```

```
dn: CN=TGtransfer1,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGtransfer1
description: TightGate-Pro Transfergruppe 1
sAMAccountName: TGtransfer1

dn: CN=TGtransfer2,CN=Users,DC=SSO,DC=M-PRIVACY,DC=HOM
objectClass: top
objectClass: group
cn: TGtransfer2
description: TightGate-Pro Transfergruppe 2
sAMAccountName: TGtransfer2
```

7.2.5 Einlesen der AD-Sicherheitsgruppen

Nach Anpassung der Konfigurationsdatei im Texteditor ist diese abzuspeichern und in den AD-Server einzulesen. Hierzu kann die Windows Power Shell verwendet werden. Der erforderliche Befehl lautet:

```
ldifde.exe -i -f [Dateiname].ldf -s [DNS-Name des ADS].[Domäne des ADS]
```

In unserem Beispiel (mit den beispielhaften Parametern) zur Veranschaulichung:

```
Bsp: ldifde.exe -i -f tgpro.ldf -s win2008.sso.m-privacy.hom
```

7.2.6 AD-Berechtigungen zuweisen

Nachdem die AD-Sicherheitsgruppen bestehen, können Benutzer auf dem AD-Server wie gewohnt diesen Gruppen zugeordnet werden. Sie erhalten dann automatisch auf TightGate®-Pro Server die entsprechenden Berechtigungen, die durch die jeweilige Gruppe repräsentiert werden. Gruppen können rekursiv definiert werden, das heißt, Gruppen können Mitglied in Gruppen sein. Hierdurch ist eine indirekte Gruppenzugehörigkeit für Benutzer realisierbar.

Nachfolgende Übersicht gibt die mit den verschiedenen Gruppen verbundenen Berechtigungen wieder:

Gruppenname	Berechtigung auf TightGate®-Pro Server
TGProUser	Benutzung von TightGate®-Pro Server (Login, Internetnutzung)
TGtransfer	Verwendung der Dateischleuse **Hinweis:** Die Berechtigung kann über diese Gruppe nur erteilt oder entzogen werden. Eine weitergehende Konfiguration hinsichtlich möglicher Übertragungsrichtungen und erlaubter Dateitypen ist in der Benutzerverwaltung von TightGate®-Pro Server möglich.
TGaudio	Übertragung von Audiosignalen zum Klienten
TGadminMaint	Anmeldung als Administrator ***maint***
TGadminConfig	Anmeldung als Administrator ***config***
TGadminUpdate	Anmeldung als Administrator ***update***
TGadminBackuser	Anmeldung als Administrator ***backuser***
TGadminRoot	Anmeldung als Administrator ***root***
TGadminSecurity	Anmeldung als Administrator ***security***
TGprivileged	Benutzung von TightGate®-Pro Server (Login, Internetnutzung) als privilegierter Benutzer (spezieller Lizenzpool)
TGunfiltered	Benutzung von TightGate®-Pro Server (Login, Internetnutzung) bei deaktiviertem Inhaltsfilter

Gruppenname	Berechtigung auf TightGate®-Pro Server
TGtransferSpool	Berechtigung für die automatische Druckausgabe auf dem Windows Arbeitsplatzrechner. Zur Nutzung ist ebenfalls die Mitgliedschaft in der Gruppe TGtransfer notwendig.
TGtransfer	Berechtigung zur Verwendung der Dateischleuse **Hinweis:** Die Berechtigung zum Dateitransfer kann über diese Gruppe nur erteilt oder entzogen werden. Eine weitergehende Konfiguration hinsichtlich möglicher Übertragungsrichtungen und erlaubter Dateitypen ist über die Gruppen TGtransfer1 bis TGtransfer99 möglich.
TGtransfer1	Transfergruppe 1 zur Definition erlaubter MIME-TYPEN für den Dateitransfer. Die Mitgliedschaft in der Gruppe TGtransfer ist zu Nutzung obligatorisch.
TGtransfer2	Transfergruppe 2 zur Definition erlaubter MIME-TYPEN für den Dateitransfer. Die Mitgliedschaft in der Gruppe TGtransfer ist zu Nutzung obligatorisch. Es können bis zu 99 Transfer-Gruppen definiert werden.

7.2.7 Authentisierungsschlüssel für TightGate®-Pro Server erzeugen

Damit sich TightGate®-Pro Server am AD-Server authentisieren kann, benötigt ersterer ein spezielles Zertifikat, das in einer sogenannten keytab-Datei enthalten ist. Diese keytab-Datei wird einmalig auf dem AD-Server unter Angabe bestimmter Parameter erzeugt und TightGate®-Pro Server zur Verfügung gestellt.

Der Befehl **für Einzelsysteme** auf dem AD-Server zur Erzeugung der keytab-Datei wird über die Windows Power Shell abgesetzt und hat folgendes Format:

```
ktpass.exe /out [Dateiname]
/mapuser [Computer-Name von TG-Pro]$@[ADS-REALM]
/princ host/[Computer-Name von TG-Pro].[Domäne TG-Pro]@[ADS-REALM]
/rndPass /crypto AES256-SHA1 /ptype KRB5_NT_SRV_HST
```

Der Befehl **für Clustersysteme (Verbundrechner)** auf dem AD-Server zur Erzeugung der keytab-Datei hat folgendes Format:

```
ktpass.exe /out [Dateiname]
/mapuser [Computer-Name von TG-Pro Cluster]$@[ADS-REALM]
/princ host/[Domäne TG-Pro Clust.]@[ADS-REALM] /rndPass /crypto AES256-
SHA1 /ptype KRB5_NT_SRV_HST
```

Achtung: Der Befehl ist ohne Zeilenumbrüche und lediglich mit Leerzeichen zwischen Schlüsselworten und Parametern einzugeben. Die Groß-/Kleinschreibung ist unbedingt zu beachten.

Folgende Übersicht erläutert die Bedeutung der Parameter bei der Erzeugung der keytab-Datei:

Schlüsselwort	Beschreibung	Beispielwert
/out	Name der Ausgabedatei. **Achtung:** Dieser Dateiname muss immer mit .keytab enden.	TGPro.keytab
/mapuser	Spezifiziert das Zielsystem, für das die erzeugte keytab-Datei gelten soll, in diesem Fall TightGate®-Pro Server, im Format [Computer-Name von TG-Pro]$@[ADS-REALM]	TGPRO$@ SSO.M-PRIVACY.HOM
/princ	Spezifiziert den Principal-Namen im Format	**Für Einzelsysteme:** host/TGPro.sso.m-privacy. hom@SSO.M-PRIVACY.HOM **Für Clustersysteme:** host/cluster.internet.netz@S-SO.M-PRIVACY.HOM
/rndPass	Zufällig vom System erzeugtes Passwort.	Es muss kein Wert gesetzt werden.
/crypto	Spezifiziert die Schlüssel, welche in der keytab-Datei eingebettet werden. **Achtung:** Nur der kryptografische Typ AES256-SHA1 wird von TightGate®-Pro Server unterstützt.	AES256-SHA1
/ptype	Spezifiziert den Prinzipal-Typ, es wird nur der HOST-Service benötigt. **Achtung:** Es muss der angegebene Wert gesetzt werden.	KRB5_NT_SRV_HST

Die Befehlszeile **für Einzelsysteme** lautet entsprechend der beispielhaft gesetzten Werte:

```
ktpass.exe /out TGPro.keytab /mapuser TGPro$@SSO.M-PRIVACY.HOM /princ
host/TGPro.sso.m-privacy.hom@SSO.M-PRIVACY.HOM /rndPass /crypto AES256-
SHA1 /ptype KRB5_NT_SRV_HST
```

Die Befehlszeile **für Clustersysteme** lautet entsprechend der beispielhaft gesetzten Werte:

```
ktpass.exe /out srv-TGPro.keytab /mapuser srv-TGPro$@SSO.M-PRIVACY.HOM
/princ host/cluster.internet.netz@SSO.M-PRIVACY.HOM
/rndPass /crypto AES256-SHA1 /ptype KRB5_NT_SRV_HST
```

Hinweis: Die Bestätigungsfrage ist mit ***Ja / Yes*** zu beantworten.

Abschließend ist die erzeugte keytab-Datei im Transfer-Verzeichnis des Administrators ***config*** auf TightGate®-Pro Server zu hinterlegen, bis das ***Sanft Anwenden*** des folgenden, letzten Konfigurationsschritts abgeschlossen ist. Dann kann die Datei wieder aus dem Transfer-Verzeichnis des Administrators ***config*** gelöscht werden.

7.3 TightGate®-Pro Server für AD-Nutzung konfigurieren

Abschließend müssen die notwendigen Einstellungen an TightGate®-Pro Server als Administrator ***config*** vorgenommen werden. Nach Anmeldung auf der Konsole sind die Einstelloptionen unter ***config > Einstellungen > Authentisierung*** entsprechend **Abschnitt 4.5.4** dieses Administrationshandbuchs zu bearbeiten. Nachfolgende Tabelle zeigt die Belegung der betreffenden Einstelloptionen mit den angenommenen Beispielwerten zur Veranschaulichung:

7.3.1 Einstelloptionen für AD-Nutzung

config > Einstellungen > Authentisierung		
Menüpunkt	**Beispielwert**	**Bemerkung**
Zurück	Rückkehr zum Hauptmenü.	Keine Einstelloption.
Authentisierungs-Methode*	AD	Verpflichtend.
Benutzer-Zertifikate automatisch*	Nein	Nur relevant bei Nutzung der integrierten SSO-Authentisierung.
Windows-Cursor in Klienten-Konfig.	Nein	Bei Bedarf.
Benutzerverz. automatisch*	Ja	
Benutzernamen in Kleinbuchstaben*	Ja	
Lokales Passwort*	Nein	Deaktivieren.
Mehrere Transfer-Benutzer*	Nein	Bei Bedarf.
Kerberos Realm*	SSO.M-PRIVACY.HOM	Domäne des AD-Servers (ADS-REALM).
Kerberos KDC 1*	192.168.4.208	IPv4-Adresse des AD-Servers.
Kerberos KDC 2*		Dto, bei Bedarf.
Kerberos Admin Server*	192.168.4.208	IPv4-Adresse des AD-Servers.
Kerberos Hostname*	TGPro (für Einzelsystem) cluster.internet.netz (für Clustersystem)	DNS-Name von TightGate®-Pro Server. Nicht den Namen des AD-Servers angeben!
Kerberos Service	host	Keine Einstelloption.
Importiere Kerberos Host Keytab	TGPro.keytab	Abgelegte keytab-Datei auswählen. Kann nach ***Speichern*** und ***Sanft Anwenden*** wieder auf dem Transfer-Verzeichnis des Administrators ***config*** entfernt werden.
Transfer-MIME-Typen-Gruppen	2	Anzahl der Transfer-Gruppen. Siehe Verwendungshinweis im Anschluss an diese Tabelle.
LDAP Base*	dc=sso, dc=m-privacy, dc=hom	Bestandteile der Domain des AD-Servers (ADS-REALM)
LDAP Server-Netzwerke*	192.168.4.0/24	IPv4-Adresse des / der LDAP-Server/s
LDAP Server 1*	192.168.4.208/32	IPv4-Adresse des ersten LDAP-Servers.
LDAP Server 2*		IPv4-Adresse des zweiten LDAP-Servers, falls vorhanden.

7.3.2 Nutzung der TGtransfer-Gruppen

Die Nutzung der TGtransfer-Gruppen erfolgt folgendermaßen:

1. Die Anzahl der gewünschten Transfer-Gruppen festlegen (Maximal 99)
2. Nach der Auswahl der Anzahl stehen entsprechend viele Gruppen zur Konfiguration bereit. Durch Auswahl der einzelnen Gruppe können die gewünschten erlaubten MIME-Typen zugewiesen werden.

Hinweis: Die Zuweisung, welche User in den jeweiligen Transfer-Gruppen sind, erfolgt durch Zuweisung der User in die Sicherheitsgruppen im AD. Ist ein Benutzer in mehreren Transfer-Gruppen so addieren sich die Transferberechtigungen der einzelnen Gruppen.

Achtung: Um TightGate®-Pro Server zur Nutzung mit einem Active Directory umzuschalten, sind alle Änderungen in vorstehender Konfiguration zu ***Speichern*** und anschließend mit ***Sanft Anwenden*** zu aktivieren. zuvor müssen alle Einstellungen am AD-Server vollzogen und die keytab-Datei im Transfer-Verzeichnis des Administrators ***config*** hinterlegt worden sein.

7.3.3 Überprüfung der Einstellungen

Die Korrektheit der Einstellungen bei der Nutzung eines Active Directory kann als Administrators ***config*** über den Menüpunkt ***Netzwerk prüfen*** kontrolliert werden. Nur wenn folgende Tests mit OK durch das System bestätigt wurden, sind die Voraussetzungen am TightGate-Pro gegeben:

Testname	Ergebnis
Tests System name in DNS / UDP:	OK
System name im DNS / TCP:	OK
----	OK
KRBKDC1 mit TCP:	OK
KRBKDC1 IP DNS reverse:	OK
KRBKDC1 DNS forward:	OK
KRBKDC1 DNS = IP:	OK
Keytab Principal with SSL CN:	OK
LDAP Server 1:	OK
LDAP1 IP DNS reverse:	OK
LDAP1 DNS forward:	OK
LDAP1 DNS = IP:	OK
LDAP1 test SASL mech query:	OK
LDAP1 supports GSSAPI:	OK
Timeserver 1:	OK

7.4 Hinweise zur Systemadministration via SSH

Unter bestimmten Umständen kann es zu einer starken Verzögerung bei der Anmeldung an einem Administrationskonto per SSH kommen, falls zugleich die Authentisierungsmethode von TightGate®-Pro Server auf „AD“ eingestellt ist. Um diese Situation zu vermeiden, muss die Reihenfolge der Authentisierungsverfahren im SSH-Klient den tatsächlichen Gegebenheiten entsprechen. Wird der Login per SSH nicht über Active Directory (AD), sondern mit einem separaten Key vollzogen, darf beispielsweise nicht GSSAPI vor AD in der jeweiligen Konfigurationsdatei des SSH-Klienten eingetragen sein. Andernfalls

kommt es durch die Wartezeit auf eine nicht funktionale Authentisierung zu den genannten Verzögerungen bei der Anmeldung. Die Konfigurationsdatei ***~/.ssh/config*** ist zu diesem Zweck um folgende Zeile zu ergänzen:

```
PreferredAuthentications publickey,keyboard-interactive,gssapi-with-mic
```

Dadurch wird die Public-Key-Authentisierung und die manuelle Passworteingabe dem AD-Ticket-Login vorgezogen.

8 Texttransfer über die Zwischenablage

Um Text im Unicode-Format sicher zwischen TightGate®-Pro Server und dem Arbeitsplatzrechner auszutauschen, kann die Zwischenablage genutzt werden. Dabei wird ein Text mit der Maus markiert, per Kontextmenü oder Tastenkombination in die Zwischenablage kopiert und anschließend aus der Zwischenablage auf dem Arbeitsplatzrechner wieder eingefügt. Dieser Texttransfer über die Zwischenablage funktioniert auch in umgekehrter Richtung.

Achtung: Über die Zwischenablage wird nur Text im Unicode-Format übertragen. Es ist nicht möglich, Programme oder Bilder über die Zwischenablage auszutauschen. Auch Formatierungen gehen beim Transfer verloren. Zum Dateitransfer ist die Dateischleuse zu nutzen.

Hinweis: Die Zwischenablage unterstützt die vielseitige UTF-8-Kodierung. Damit können beliebige Sonderzeichen übertragen werden, die der VNC-Klient anfordert.

8.1 Generelles zur Nutzung der Zwischenablage

Die generelle Voreinstellung der Zwischenablage kann systemweit kontrolliert werden. Diese Voreinstellungen werden über den Administrator ***config*** vorgenommen

config > Einstellungen > Zwischenablage		**Hinweise**		
Menüoption	**Beschreibung**	**C**	**E**	**F**
Keine	Die Zwischenablage wird serverseitig deaktiviert. Ein Transfer von Textdaten ist in keine Richtung möglich. **Hinweis:** Für TightGate®-Pro (CC) Version 1.4 Server ist dies die Werkseinstellung. Diese kann jedoch geändert werden.			
Server zu Klient	Textdaten können über die Zwischenablage nur von TightGate®-Pro Server auf den Arbeitsplatzrechner übertragen werden.			
Klient zu Server	Textdaten können über die Zwischenablage nur vom Arbeitsplatzrechner auf TightGate®-Pro Server übertragen werden.			
Voll-duplex	Textdaten können über die Zwischenablage in beide Richtungen übertragen werden			

8.2 Nutzung der Zwischenablage mit Einzelbestätigung

Der Texttransfer über die Zwischenablage kann so konfiguriert werden, dass jede einzelne Übertragung vom Benutzer explizit zu bestätigen ist. Die CC-konforme Fassung des Viewer-Programms (TightGate®-Pro (CC) Version 1.4 Client) kann auch mit der nicht CC-konformen Fassung von TightGate®-Pro Server eingesetzt werden, sofern die Nutzung der Zwischenablage mit Einzelbestätigung gewünscht wird. In CC-konformen Umgebungen ist zusammen mit TightGate®-Pro (CC) Version 1.4 Server ausschließlich TightGate®-Pro (CC) Version 1.4 Client zu verwenden, bei dem die Nutzung der Zwischenablage mit Einzelbestätigung voreingestellt ist.

8.2.1 Benutzerseitige Vorarbeiten (falls nötig)

Hinweis: In der CC-konformen Fassung des Viewer-Programms (TightGate®-Pro (CC) Version 1.4 Client) ist diese Form des bestätigten Transfers über die Zwischenablage bereits werkseitig voreingestellt.

Achtung: Für TightGate®-Pro (CC) Version 1.4 Server ist der Transfer via Zwischenablage serverseitig in der Werkseinstellung generell deaktiviert. Dieses Verhalten kann jedoch über den Administrator ***config*** geändert werden (siehe oben).

Die Einstellung einer fallweisen Bestätigung des Texttransfers über die Zwischenablage ist im Optionsmenü des Viewer-Programms auf dem Arbeitsplatzrechner vorzunehmen. Es ist über die Funktionstaste F8 konfigurierbar. Nach Wahl des Menüpunkts ***Optionen …*** wird das Optionsmenü ange-

zeigt. Im Reiter ***Eingabe*** sind hierzu die Kontrollkästchen ***Clipboard an Server senden*** und ***Clipboard vom Server annehmen*** zu deaktivieren. Schließlich ist die geänderte Einstellung im Reiter **Laden / Speichern** zu speichern. Anschließend muss der Viewer geschlossen und erneut geöffnet werden.

Anschließend befinden sich im Optionsmenü des Viewer-Programms zwei weitere Felder: ***Zwischenablage vom Server*** und ***Zwischenablage an Server***. Hiermit können Textinhalte fallweise aus der Zwischenablage von TightGate®-Pro Server in die Zwischenablage des lokalen Arbeitsplatzes abgeholt oder umgekehrt von der Zwischenablage des lokalen Arbeitsplatzes in die Zwischenablage von TightGate®-Pro Server übertragen werden. Die Anwahl der jeweiligen Option gilt immer nur für eine Operation. Zur Übertragung weiterer Inhalte ist die jeweilige Option erneut zu wählen.

Hinweis: Die zusätzlichen Optionen werden im Optionsmenü des Viewer-Programms nicht angezeigt, wenn automatischer Austausch der Zwischenablagen aktiviert ist.

8.2.2 Vorgehensweise zum Transfer von TightGate®-Pro Server auf den Windows-Klienten

1. Text durch Selektion oder manuell über den Menübefehl ***Kopieren*** in die serverseitige Zwischenablage einlesen.
2. Durch ***Funktionstaste F8 > Receive Clipboard*** im Viewer-Programm die Übertragung in die Windows-Zwischenablage bestätigen.
3. Aufseiten des Windows-Klienten Text durch Tastenkombination oder Menübefehl ***Einfügen*** an der gewünschten Stelle einfügen.

8.2.3 Vorgehensweise zum Transfer vom Windows-Klienten auf TightGate®-Pro Server

1. Text durch Selektion oder manuell über den Menübefehl ***Kopieren*** in die klientenseitige Zwischenablage einlesen.
2. Durch ***Funktionstaste F8 > Send Clipboard*** im Viewer-Programm die Übertragung in die Zwischenablage von TightGate®-Pro Server bestätigen.
3. Aufseiten von TightGate®-Pro Server den Text durch Tastenkombination oder Menübefehl ***Einfügen*** an der gewünschten Stelle einfügen.

Hinweis: Anstelle der Funktionstaste F8 bewirkt auch ein Rechtsklick auf die Titelleiste des Viewer-Programms die Einblendung des Optionsmenüs.

Achtung: Bei systemweit aktiviertem Texttransfer über die Zwischenablage kann die fallweise Bestätigung eines Transfers jederzeit mit der beschriebenen Verfahrensweise durch den Benutzer ab- oder zugeschaltet werden. Die jeweilige Einstellung wird nur für die Dauer der Benutzersitzung gespeichert und fällt beim Neustart des Viewer-Programms auf die serverseitige Vorgabe zurück. In CC-konformen Umgebungen darf zur Wahrung der CC-Konformität von der Verfahrensweise der Einzelbestätigung nicht abgewichen werden! Erforderlichenfalls sind die Benutzer durch geeignete organisatorische Maßnahmen auf Beibehaltung einer bestimmten Einstellung zu verpflichten.

9 Datensicherung

Datensicherung (Backup) ist mit TightGate®-Pro Server auf verschiedenen Wegen möglich. Die Administratorenrolle im Zusammenhang mit Backup-Aktivitäten heißt ***backuser***.

Besonderheiten der Datensicherung bei TightGate®-Pro Server:

- Lokale Speicherung der Datensicherung auf TightGate®-Pro Server mit Ablage der Sicherungsdateien im Verzeichnis /home/backuser/backup des Administrators ***backuser***.
  Dieses Backup wird bei jeder Sicherung automatisch erstellt. Es verbleibt an seinem Speicherort, bis es entweder manuell oder nach Erreichen des Verfalldatums automatisch gelöscht wird.
- Datensicherung auf USB-Massenspeicher
- Datensicherung über das Netzwerk auf Backup-Server

9.1 Sicherungsumfang

Die vollständige Systemkonfiguration einschließlich der Parameter aller Einstelloptionen der Administratorenzugänge von TightGate®-Pro Server werden bei einem Backup in jedem Fall auf das Sicherungsmedium geschrieben. Weitere Bestandteile sind abhängig von der Einstellung unter ***backuser > Konfiguration > Backup-Typ***. Hierdurch kann das Verhältnis aus Sicherungstiefe und Speicherplatz- / Zeitbedarf zur Sicherung bzw. Wiederherstellung den betrieblichen Erfordernissen angepasst werden.

Generell nicht gesichert werden

- Programm- und Systemdateien, die Bestandteil der Installationspakete für TightGate®-Pro Server sind, und
- Konfigurationsdaten der Add-ons für den Webbrowser, die vom Benutzer installiert wurden.

9.2 Die Konfiguration des Backups

Zur Konfiguration des Backups ist die Anmeldung als ***backuser*** an TightGate®-Pro Server erforderlich.

Hinweis: Je nach Einstellung des Hochlade-Verfahrens werden zusätzliche Einstelloptionen eingeblendet. Diese sind in nachfolgender Tabelle untereinander aufgeführt. Mitunter sind je nach Konfiguration des Hochlade-Verfahrens jedoch nicht alle Optionen zugleich sichtbar.

backuser > Konfiguration		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Zurück	Rückkehr zum Hauptmenü.		**E0**	
Speichern	Vorgenommene Änderungen werden erst nach dem Speichern wirksam.		**E0**	**F0**
Lebensdauer	Lebensdauer der Backups in Tagen. Mögliche Werte sind 0 bis nahezu unendlich. Es ist sinnvoll, die Lebensdauer in Abhängigkeit der Häufigkeit der Backups einzustellen.		**E6**	**F6**
Häufigkeit	Häufigkeit automatischer Backups. Aus Sicherheitsgründen empfiehlt es sich, täglich Backups zu erstellen.		**E1**	
Backup-Typ	Auswahl des Sicherungsumfangs.		**E1**	
Backup-Part.-Label	Bezeichnung eines USB-Laufwerkes, vgl. „Sicherung eines Backups auf einer externen USB-Festplatte“.		**E4**	
Backup-Part.-TTL	Verbleibdauer eines Backups auf dem USB-Laufwerk. Bei dem Wert 0 wird jedes vorher abgelegte Backup gelöscht.		**E6**	**F6**
Backup-Partitionen	Anzeige aller auf dem System verfügbaren Geräte.		**E0**	

backuser > Konfiguration		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Hochlade-Verfahren	Auswahl des Übertragungsverfahrens bei Dateisicherung auf einem Backup-Server: 1) SCP – verschlüsselt 2) SFTP – verschlüsselt. **Hinweise:** Je nach Einstellung des Hochlade-Verfahrens werden zusätzliche Einstelloptionen eingeblendet. Diese sind in dieser Tabelle fortlaufend untereinander aufgeführt. Mitunter sind je nach Konfiguration des Hochlade-Verfahrens jedoch nicht alle Optionen zugleich sichtbar. Die automatische Anmeldung an SCP/SFTP-Server erfolgt über den SSH-Schlüssel. Unverschlüsseltes FTP wird nicht unterstützt.		**E1**	
SSH-Schlüssel zurücksetzen	Das System wird werksseitig ohne SSH-Schlüssel ausgeliefert. In diesem Fall kann ein SSH-Schlüssel über diese Menüoption erzeugt werden. **Hinweis:** Falls bei Nutzung der Hochlade-Verfahren SCP und SFTP ist kein SSH-Schlüssel vorliegt, muss ein Passwort eingegeben werden.		**E2**	
SSH-Schlüssel anzeigen	Anzeige des bestehenden SSH-Schlüssels. Verlassen des Ansichtsmodus mit ***Enter***. Der SSH-Schlüssel kann kopiert und beispielsweise in Konfigurationsdateien eingefügt werden.		**E0**	
SSH-Schlüssel hochladen	Ablage des erzeugten SSH-Schlüssels im Verzeichnis für die abzulegenden Sicherungsdaten („Fernes Verzeichnis“).		**E0**	
Server	Auswahl des Servers für die Datensicherung. Es erscheinen nur Rechner in der Auswahlliste, die zuvor durch den Administrator ***config*** in der Netzwerkkonfiguration gesetzt wurden. Der Administrator ***backuser*** kann keine neuen Backup-Server hinzufügen oder bestehende ändern.		**E1**	
Benutzer	Benutzername zur Authentisierung am Backup-Server vor dem Hochladen der Sicherungsdateien. **Hinweis:** Im Home-Verzeichnis des Benutzers auf dem Backup-Server kann in der Datei ~/.ssh/authorized_keys ein SSH-Schlüssel hinterlegt werden, der zum Hochladen von Backup-Dateien von TightGate®-Pro Server zulässig sein soll. Wird derselbe Schlüssel dann auch in dem Verzeichnis hinterlegt, in dem die Sicherungsdaten abgelegt werden („Fernes Verzeichnis“), erfolgt bei der Verbindung zum Backup-Server keine Passwortabfrage. **Achtung:** Dieses Vorgehen ist Voraussetzung für automatische Backups von TightGate®-Pro Server mittels der Hochlade-Verfahren SCP oder SFTP.		**E4**	
Fernes Verzeichnis	Absoluter Verzeichnispfad zur Ablage der Sicherungsdateien auf dem Backup-Server. **Achtung:** Wenn Backups automatisiert mit den Hochlade-Verfahren SCP oder SFTP geschrieben werden sollen, muss zwingend ein hierfür erzeugter SSH-Schlüssel ebenfalls in diesem Verzeichnis abgelegt werden. Dies kann über die Menüoption ***SSH-Schlüssel hochladen*** erfolgen. Im Home-Verzeichnis des Benutzers auf dem Backup-Server ist in der Datei ~/.ssh/authorized_keys derselbe SSH-Schlüssel zu hinterlegen. Dieses Vorgehen ist Voraussetzung für automatische Backups von TightGate®-Pro Server mittels der Hochlade-Verfahren SCP oder SFTP.		**E4**	

backuser > Konfiguration		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
GnuPG-Schlüssel	Kennung (ID) des öffentlichen Schlüssels, mit dem das Backup verschlüsselt werden soll. Der betreffende Schlüssel muss bereits im System vorliegen, vgl. Abschnitt 9.3.3 Verschlüsselte Backups.		**E4**	
Neuer GnuPG-Schlüssel	Möglichkeit zum Einspielen eines neuen GnuPG-Schlüssels, vgl. Abschnitt 9.3.3 Verschlüsselte Backups.		**E1**	
Lösche GnuPG-Schlüssel	Möglichkeit zum Löschen nicht weiter benötigter Schlüssel. **Hinweis:** Verwendete Schlüssel können nicht gelöscht werden.		**E2**	

Achtung: Alle Änderungen müssen über den Menüpunkt ***Speichern*** gesichert werden. Andernfalls werden sie nicht wirksam.

9.3 Backup erstellen

Zur Erstellung eines Backups von TightGate®-Pro Server ist die Anmeldung als Administrator ***backuser*** in der Konsole erforderlich. Nach Konfiguration der Datensicherung sollte ein erstes Backup manuell gestartet werden, auch wenn später zu automatischen Backups übergegangen wird.

Die Datensicherung kann manuell unter dem Menüpunkt Backup gestartet werden. TightGate®-Pro Server akkumuliert alle für die Sicherung relevanten Daten und erstellt eine Sicherungsdatei. Nach Abschluss dieses Vorgangs wird die Sicherungsdatei auf das ausgewählte Medium geschrieben oder auf den Backup-Server übertragen.

Hinweis: Auf dem TightGate®-Pro Server verbleibt in jedem Fall eine lokale, unverschlüsselte Kopie der Sicherungsdatei. Aus dieser können Benutzer ihre Daten in Eigenregie wiederherstellen. Der Zugriff erfolgt nur durch ein spezielles Rücksicherungsprogramm, ein anderweitiges Lesen des Backups durch Benutzer oder Administratoren ist nicht möglich.

9.3.1 Datensicherung auf einem Backup-Server

Datensicherung auf einem Backup-Server hat den Vorteil der Standortunabhängigkeit. Günstig sind Sicherungsorte in räumlicher Trennung zum TightGate®-Pro Server. Sicherungsdateien auf entfernten Backup-Servern sollten stets verschlüsselt sein.

Im Vorfeld der Datensicherung auf einem Backup-Server wird nach Anmeldung als Administrator ***config*** im Menü ***Einstellungen*** unter ***Backup-Server*** der auflösbare Rechnername oder die IPv4-Adresse des vorgesehenen Backup-Servers hinterlegt.

Hinweis: Soll das Backup auf einen FTP-Server geschrieben werden, der sich im Bereich des Klienten-Netzwerks befindet, so muss der Backup-Server zusätzlich in die Liste der erlaubten FTP-Server unter dem Menüpunkt ***FTP ausgehend*** eingetragen werden.

Achtung: Die Einstellungen müssen mit ***Speichern*** gesichert werden. Sie werden erst nach Bestätigung von ***Sanft Anwenden*** wirksam.

Die weiteren Einstellungen erfolgen als Administrator ***backuser*** im Menü ***Konfiguration:***

1. Menüpunkt ***Hochlade-Verfahren***: Auswahl des Verfahrens für die Datenübertragung. Beispiel: SFTP.
2. Menüpunkt ***Server***: Auswahl des Backup-Servers. Hinzufügen oder Neuanlage von Backup-Servern vgl. Abschnitt 4.4.1 Einstellungen für TightGate®-Pro Server.
3. Menüpunkt ***Benutzer***: Benutzername am Backup-Server.
4. Menüpunkt ***Fernes Verzeichnis***: Pfad der Sicherungsdatei (Speicherort) auf dem Backup-Server).
5. Menüpunkt ***SSH-Schlüssel zurücksetzen***: Bei Bedarf SSH-Schlüssel ersetzen oder erzeugen. Anschließend ***SSH-Schlüssel hochladen*** wählen, um den Schlüssel im entfernten Verzeichnis auf dem Backup-Server abzulegen.

6. Im Home-Verzeichnis des Benutzers auf dem Backup-Server ist in der Datei ~/.ssh/authorized_keys derselbe SSH-Schlüssel zu hinterlegen. Der SSH-Schlüssel kann zu diesem Zweck über ***SSH-Schlüssel anzeigen*** am Bildschirm angezeigt und von dort kopiert werden.
7. Menüpunkt ***Speichern***: Sicherung der Konfiguration.
8. Menüpunkt ***backuser > Backup***: Start der Datensicherung.

Es empfiehlt sich, die korrekte Datensicherung auf dem Backup-Server manuell zu überprüfen.

9.3.2 Sicherung eines Backups auf einer externen USB-Festplatte

Für die Sicherung eines Backups auf einer USB-Festplatte sind einige Vorarbeiten notwendig. Zunächst muss für die USB-Festplatte ein Label-Name vergeben werden.

Achtung: Für den Fall, dass mehrere Festplatten zum Einsatz kommen, müssen diese alle denselben Label-Namen erhalten. Jede USB-Festplatte muss zum Einsatz mit TightGate®-Pro Server mit dem Dateisystem ext (extended) formatiert sein. Da dies ein auf Linux basierendes Dateiformat ist, bezieht sich die folgende Anleitung zur Vorbereitung der Festplatten auf eine Linux-Distribution. Nach Vorbereitung der Festplatten (siehe unten) ist TightGate®-Pro Server einzurichten.

Die folgenden Schritte setzen die Anmeldung als ***backuser*** voraus. Im Menü ***Konfiguration*** sind die folgenden Operationen auszuführen:

1. Menüpunkt ***Backup-Part.-Label***: Eintrag des Label-Namens, d. h. der Bezeichnung der externen Festplatte.
2. Menüpunkt ***Backup-Part.-TTL***: Eintrag der Aufbewahrungszeit der Sicherungsdateien auf der USB-Festplatte.
3. Menüpunkt ***Speichern***: Sicherung der Einstellungen.
4. Verbindung der USB-Festplatte mit TightGate®-Pro Server.
5. Menüpunkt ***backuser > Backup***: manueller Start der Datensicherung.

Es empfiehlt sich, die korrekte Datensicherung auf der USB-Festplatte manuell zu überprüfen.

Zur Festplattenvorbereitung unter Linux sind ***root***-Rechte erforderlich. Die folgenden Schritte werden auf der Konsole ausgeführt.

1. Nach Anschluss des Laufwerks an den USB-Port von TightGate®-Pro Server wird eine Laufwerksbezeichnung (Device) vergeben. Anlegen einer Partition vom Typ Linux mit dem Befehl ***fdisk /dev/sdb***
   Die Laufwerksbezeichnung „sdb“ kann abweichen. Es ist die korrekte Bezeichnung entsprechend der Systemvorgabe anzugeben. Die Parameter ermöglichen die folgenden Aktionen:
   p Anzeige der momentanen Partitionstabelle
   d Löschen der Partition
   n Anlegen der Partition
   w Speicherung der neuen Partitionstabelle und Beenden von fdisk

2. Zur Formatierung der Platte dient der Befehl
   mke2fs -j -L TG-Backup /dev/sdb1
   Die Partitionsbezeichnung „sdb1“ kann abweichen. Es ist die korrekte Bezeichnung entsprechend der Systemvorgabe anzugeben. Mit „TG-Backup“ wird in diesem Fall das Label bezeichnet, das dann auch in der Konfiguration von TightGate®-Pro Server als Administrator ***backuser*** zu referenzieren ist.
   Achtung: Für den Fall, dass mehrere Festplatten zum Einsatz kommen, müssen diese alle den gleichen Labelnamen haben!

3. Abschalten des Festplattenchecks mit dem Befehl
   tune2fs -i 0 /dev/sdb
   Die Laufwerksbezeichnung „sdb“ kann abweichen. Es ist die korrekte Bezeichnung entsprechend der Systemvorgabe anzugeben.

9.3.3 Verschlüsselte Backups

Um den unbefugten Zugriff auf externe Backups zu verhindern, können diese mit einem GnuPG-Key verschlüsselt werden. Dafür muss dem Administrator ***backuser*** der öffentliche Schlüssel eines GnuPG-Schlüsselpaares zur Verfügung stehen. Der öffentliche GnuPG-Key muss zu diesem Zweck via SCP in das Verzeichnis “keys” des Administrators ***backuser*** kopiert werden.

Achtung: Bei TightGate®-Pro (CC) Version 1.4 Server muss der öffentliche GnuPG-Key stattdessen in das sogenannte Shared Storage unter home/user/.transfer/backuser kopiert und von dort abgeholt werden, da ein direktes Kopieren des Schlüssels in CC-konformen Umgebungen nicht zulässig ist.

Hinweis: Weitere Informationen zu GnuPG und zur Funktionsweise asymmetrischer Verschlüsselung sind unter http://www.gnupg.org/ verfügbar.

Die folgenden Schritte setzen die Anmeldung als ***backuser*** voraus. Im Menü ***Konfiguration*** sind die folgenden Operationen auszuführen:

1. Menüpunkt ***Neuer GnuPG-Schlüssel***: Import des zu verwendenden Schlüssels. Sollte bereits ein Schlüssel importiert sein, ist dieser Schritt nicht unbedingt erforderlich.
2. Menüpunkt ***GnuPG-Schlüssel***: Auswahl des zu verwendenden Schlüssels.
3. Menüpunkt ***Speichern***: Sicherung der Einstellungen.
4. Menüpunkt ***backuser > Backup***: manueller Start der Datensicherung.

Es empfiehlt sich, die Datensicherung auf dem Backup-Server manuell zu überprüfen.

Hinweis: Auf TightGate®-Pro Server verbleibt in jedem Fall eine lokale, unverschlüsselte Kopie der Sicherungsdatei. Aus dieser können Benutzer Daten in Eigenregie wiederherstellen. Der Zugriff erfolgt nur durch ein spezielles Rücksicherungsprogramm, ein anderweitiges Lesen des Backups durch Benutzer oder Administratoren ist nicht möglich.

9.3.4 Protokollauswertung des automatischen Backups

Zur nachträglichen Analyse automatischer Sicherungsläufe werden Protokolldateien erstellt. Diese können über den Menüpunkt ***backuser > Letztes Protokoll anzeigen*** eingesehen werden. Für manuell ausgelöste Sicherungsläufe wird kein Protokoll erstellt.

9.4 Rücksicherung eines Backups

Der Administrator ***backuser*** ist lediglich für die Erstellung der Backups, jedoch nicht für deren Rücksicherung zuständig. Die Wiederherstellung gesicherter Daten aus einem Backup-Satz erfolgt durch den Administrator ***config*** für die Systemkonfiguration und durch den Administrator ***maint*** für die Benutzerkonten. Zusätzlich hat jeder Benutzer die Möglichkeit, seine eigenen Daten nach Bedarf aus den Backup-Sätzen wiederherzustellen, die zu diesem Zeitpunkt im Verzeichnis /home/backuser/backup des Administrators ***backuser*** vorgehalten werden.

Eine vollständige Wiederherstellung von TightGate®-Pro Server, beispielsweise nach einer Neuinstallation, umfasst die Rücksicherung der Systemkonfiguration sowie die Rücksicherung der Benutzerkonten.

Hinweis: Es wird in jedem Fall bei jeder Erstellung einer Datensicherung zunächst ein Backup-Satz lokal auf TightGate®-Pro Server angelegt. Dieser ist stets unverschlüsselt und liegt im Verzeichnis /home/backuser/backup des Administrators ***backuser***. Jede Rücksicherung kann nur aus diesem Verzeichnis oder direkt von einer USB-Festplatte erfolgen. Daten, die verschlüsselt und auf USB-Festplatte oder auf einen externen Backup-Server übertragen wurden, müssen vor der weiteren Verarbeitung manuell entschlüsselt werden. Der hierzu notwendige private Schlüssel befindet sich regelmäßig nicht auf TightGate®-Pro Server, sondern ist extern bereitzustellen.

9.4.1 Wiederherstellung der Systemkonfiguration

Die Systemkonfiguration wird durch den Administrator ***config*** aus einem Backup-Satz (Datesicherungsdatei) wiederhergestellt. Dieser kann sich lokal auf TightGate®-Pro Server im Verzeichnis /home/backuser/backup des Administrators ***backuser*** oder auf einer angeschlossenen USB-Festplatte befinden.

Zur Wiederherstellung der Systemkonfiguration ist eine Anmeldung als ***config*** an der Konsole erforderlich. Unter dem Menüpunkt ***config > Einstellungen > Wiederherstellen*** kann die Quelle für Sicherungsdateien (Backup-Sätze) gewählt werden. Dies kann das Verzeichnis /home/backuser/backup des Administrators backuser auf der lokalen Festplatte von TightGate®-Pro Server sein oder eine externe USB-Festplatte.

Hinweis: Verschlüsselt abgelegte Backup-Sätze sind vor der Rücksicherung manuell zu entschlüsseln.

Nach Auswahl des gewünschten Backup-Satzes und Bestätigung einer Sicherheitsabfrage wird die Systemkonfiguration aus der Datensicherung wiederhergestellt.

Achtung: Die bisherige Systemkonfiguration wird überschrieben. Im Zweifel empfiehlt sich die Durchführung eines aktuellen Backups, um Datenverlust infolge der Rücksicherung eines falschen Backup-Satzes zu vermeiden.

Zur Rücksicherung von einem entfernten Backup-Server sind die relevanten Backup-Sätze ggf. manuell zu entschlüsseln und von einer über USB angesclossenen Festplatte oder per SFTP von einem entfernten Backup-Server in das Verzeichnis /home/backuser/backup auf TightGate®-Pro Server zu kopieren. Dort stehen sie der Wiederherstellung durch den Administrator ***config*** wie oben beschrieben zur Verfügung.

9.4.2 Wiederherstellung der Benutzerkonten

Die Benutzerkonten werden durch den Administrator ***maint*** aus einem Backup-Satz (Datensicherungsdatei) wiederhergestellt. Dieser kann sich lokal auf TightGate®-Pro Server im Verzeichnis

/home/backuser/backup des Administrators ***backuser*** oder auf einer angeschlossenen USB-Festplatte befinden.

Zur Wiederherstellung der Benutzerkonten ist eine Anmeldung als ***maint*** an der Konsole erforderlich. Unter dem Menüpunkt ***maint > Benutzerverwaltung > Regeneriere Benutzer*** kann die Quelle für Sicherungsdateien (Backup-Sätze) gewählt werden. Dies kann das Verzeichnis /home/backuser/backup des Administrators ***backuser*** auf der lokalen Festplatte von TightGate®-Pro Server sein oder eine externe USB-Festplatte. Es besteht die Möglichkeit der Auswahl aller Benutzerkonten oder einzelner Benutzerkonten zur Wiederherstellung.

Hinweis: Verschlüsselt abgelegte Backup-Sätze sind vor der Rücksicherung manuell zu entschlüsseln.

Nach Auswahl des gewünschten Backup-Satzes und Bestätigung einer Sicherheitsabfrage werden die Benutzerkonten aus der Datensicherung wiederhergestellt.

Achtung: Die bisherigen Benutzerkonten werden überschrieben. Im Zweifel empfiehlt sich die Durchführung eines aktuellen Backups, um Datenverlust infolge der Rücksicherung eines falschen Backup-Satzes zu vermeiden.

Zur Rücksicherung von einem entfernten Backup-Server sind die relevanten Backup-Sätze ggf. manuell zu entschlüsseln und per SFTP in das Verzeichnis /home/backuser/backup auf TightGate®-Pro Server zu kopieren. Dort stehen sie der Wiederherstellung durch den Administrator ***config*** wie oben beschrieben zur Verfügung.

9.4.3 Benutzerindividuelle Wiederherstellung

Jeder Benutzer hat die Möglichkeit, seine eigenen Daten über das Menü der Benutzeroberfläche des Viewers in Eigenregie aus lokal im Verzeichnis /home/backuser/backup vorgehaltenen Backup-Sätzen (Datensicherungen) wiederherzustellen.

Über ***Menü > Dienstprogramme > Daten-Wiederherstellung*** kann der gewünschte Backup-Satz und die wiederherzustellenden Daten ausgewählt werden. Nach einer Sicherheitsabfrage beginnt die Rücksicherung.

Achtung: Bestehende Daten des betreffenden Benutzerkontos werden überschrieben!

10 Aktualisierung von TightGate®-Pro Server

Die zusammen mit TightGate®-Pro erhältlichen Verträge zur Softwarepflege berechtigen innerhalb der Laufzeit zu kostenfreien Updates und Upgrades. Das System wird nach ordnungsgemäßer Lizenzierung und Registrierung auf den Update-Servern der m-privacy GmbH freigeschaltet. Sonderaufgaben des Administrators ***update*** sind die Installation von iBus-Modulen zur Eingabe von landesspezifischen Sonderzeichen sowie die Durchführung von Integritätsprüfungen (siehe unten).

Die Aktualisierung von TightGate®-Pro Server ist manuell oder zeitgesteuert möglich. In Sonderfällen können auch Teil-Updates in Absprache mit dem technischen Kundendienst der m-privacy GmbH durchgeführt werden.

Warnung: Zur Aufrechterhaltung von Schutzniveau und Betriebssicherheit wird nachdrücklich empfohlen, TightGate®-Pro Server stets auf einem aktuellen Stand zu halten. In diesem Zusammenhang sei darauf verwiesen, dass neben der Systemsoftware für TightGate®-Pro Server auch die Programmdateien für einen eventuell installierten On-Access-Malware-Scanner zur Überwachung der Dateischleuse im Zuge des automatischen Updateprozesses aktualisiert werden.

Achtung: Automatische Updates sind nur möglich, wenn auf die Update-Server der m-privacy GmbH zugegriffen werden kann. Entsprechende Einstellungen sind als Administrator ***config*** in der Netzwerk-Konfiguration unter dem Menüpunkt ***Wartung*** vorzunehmen. Die Konfiguration erfolgt in der Regel durch die m-privacy GmbH im Rahmen der Bereitstellung des Systems.

Hinweis: Die Update-Server der m-privacy GmbH sind redundant ausgelegt. Bei Ausfall des Hauptservers kann auf einen Reserveserver zugegriffen werden. Die zuverlässige Aktualisierung von TightGate®-Pro Server ist damit jederzeit gegeben. Auch die Einrichtung eines Ersatz-Update-Servers erfolgt in der Regel durch die m-privacy GmbH im Rahmen der Bereitstellung des Systems.

10.1 Registrierung zur Nutzung der Update-Server

Zur Freischaltung für das automatische Update-System muss TightGate®-Pro Server ordnungsgemäß bei der m-privacy GmbH registriert sein. Die Registrierung ist dauerhaft gültig. Sie muss nur bei einer Neuinstallation oder einem Wechsel des Update-Schlüssels erneuert werden. Zur Registrierung sind zumindest folgende Schritte notwendig:

1. Anmeldung am Login-Prompt als Administrator ***config.***
2. Ggf. Eintragung des SMTP-Mailservers zum Mailversand, ***Speichern*** und ***Sanft Anwenden.***
3. Menüpunkt ***config > Online-Reg.***: Eintrag der Lizenznummer und weiterer Angaben in das Dialogfeld.
4. Menüpunkt ***config > Online-Reg. > SSH-Schlüssel***: Erzeugung eines SSH-Schlüssels. Beenden der Schlüsselanzeige mit der Taste „q“.
5. Menüpunkt ***config > Online-Reg. > Speichern***: Sicherung der Einstellungen.
6. Menüpunkt ***config > Online-Reg. > Senden***: Versand der Registrierung an die m-privacy GmbH.

Die Registrierung wird verschlüsselt an die m-privacy GmbH versandt. Die Freischaltung für automatische Updates geschieht innerhalb von drei Werktagen und wird per E-Mail bestätigt. Danach kann das Online-Aktualisierungssystem genutzt werden.

Hinweis: Jeder Aktualisierungsprozess wird von TightGate®-Pro Server protokolliert. Über die Option ***update > Protokoll anzeigen*** im Menü des Administrators ***update*** können die Protokolle zurückliegender Update-Läufe abgerufen und im Fehlerfall geprüft werden.

10.2 Grundsätzliches zum Update-Verfahren

Die Aktualisierung von TightGate®-Pro Server besteht immer aus zwei Schritten, die konsekutiv ausgeführt werden: dem Herunterladen der Aktualisierungsdateien (Download) und der eigentlichen Aktualisierung des Systems (Update).

10.2.1 Ablauftechnische Überlegungen

Generell setzt ein Update-Lauf immer das Herunterladen der Aktualisierungsdateien voraus, dies gilt jedoch umgekehrt nicht zwingend. Aktualisierungsdateien Können auch zeitlich getrennt vor dem eigentlichen Updatelauf vom Aktualisierungsserver der m-privacy GmbH abgerufen werden. Da die Aktualiserungsdateien einen Umfang von mehreren 100 MB haben können, ist letzteres Verfahren insbesondere bei schmalbandigen Verbindungen zu den Aktualisierungsservern relevant, um das notwendige Wartungsfenster klein zu halten. Während des Downloads kann der Produktivbetrieb von TightGate®-Pro Server ungehindert weiterlaufen. Während eines Updatelaufs (Einspielen der Aktualisierungen) jedoch muss ein Einzelsystem ohne Benutzer arbeiten und auch ein zu aktualisierender Knotenrechner (Node) eines Rechnerverbunds (Cluster) muss sich im Wartungsmodus ohne Benutzer befinden.

Sowohl der Download als auch das eigentliche Update können für maximale Flexibilität im Produktivbetrieb zeitgesteuert ausgeführt werden. Damit ist es möglich, den datenintensiven Abruf der Aktualisierungsdateien in eine Zeit geringer Netzwerkbelastung zu verlegen respektive bestehende Datenkontigente optimal auszunutzen. Die eigentlichen Aktualisierungsläufe wiederum können in Zeiten mit geringem oder ohne Benutzeraufkommen geplant werden, sodass der Produktivbetrieb möglichst wenig beeinträchtigt wird.

10.2.2 Grenzen der automatischen Ablauflogik

Im Sinne der Betriebssicherheit ist es notwendig, die vorhandenen Automatiken zur Aktualisierung von TightGate®-Pro Server sinnvoll zu begrenzen. Wird ein zeitgesteuertes Update (Download inkl. Einspielung der Dateien) geplant, startet der Download der Aktualisierungsdateien unbeeinflussbar 2 Stunden vor dem eigentlich Aktualisierungslauf. Es werden maximal 10 Versuche unternommen, die notwendigen Dateien vom Aktualisierungsserver der m-privacy GmbH zu beziehen. Gelingt der Download nicht, wird ein „Warn-Merker“ gesetzt und es erfolgen unmittelbar vor dem eigentlichen Update-Lauf weitere 10 Download-Versuche. Scheitert der Download abermals, wird die Zeitsteuerung zunächst ausgeschaltet und der eigentliche Aktualisierungslauf per Update-Sperre verhindert.

Handelt es sich um den Node eines Clustersystems, schaltet sich dieser bei definitiv fehlgeschlagenem Download der Aktualisierungsdateien zusätzlich in den Wartungsmodus, der nur manuell als Administrator ***maint*** wieder deaktiviert werden kann.

Sobald der „Warn-Merker“ wegen eines fehlgeschlagenen Downloads gesetzt ist, wird der Fehlerzustand auch über Nagios mittels des Sensors *check_versions* mit der Fehlermeldung „Update download failed“ signalisiert. Weiterhin erfolgt eine entsprechende Einblendung „Update-Download-Fehler“ in der Titelleiste der Konfigurationsmenüs des Administrators ***update***. Der „Warn-Merker“ kann nur zurückgesetzt werden, indem ein vollständiger Download der Aktualisierungsdateien erfolgt.

Zur weiteren Verfahrensweise bestehen (erforderlichenfalls nach Beseitigung der Ursache für den nicht erfolgten Download der Aktualisierungsdateien) zwei Möglichkeiten:

1. Die gesetzte Update-Sperre wird über die jeweilige Konfigurationsoption des Administrators ***update*** gelöscht und danach ein manuelles oder zeitgesteurtes Update gestartet. In diesem Fall beginnt der Prozess des Downloads der Aktualisierungsdateien sofort oder zur geplanten Zeit von neuem. Bei Clustersystemen kann zuvor der Wartungsmodus manuell deaktiviert werden, damit der Node bis zum Beginn des eigentlichen Updatelaufs für Benutzer zugänglich ist.
2. Die gesetzte Update-Sperre wird über die jeweilige Konfigurationsoption des Administrators ***update*** gelöscht und ein eventuell geplantes zeitgesteuertes Update aufgehoben. Es werden dann keine Updates heruntergeladen und installiert. Bei Clustersystemen muss zudem der Wartungsmodus manuell aufgehoben werden.

Hinweis: Ein „Warn-Merker" über den gescheiterten Download kann im Gegensatz zur Update-Sperre nicht manuell gelöscht werden. Dieser hat keinen Einfluss auf den Produktivbetrieb von TightGate®-Pro Server und behindert auch nicht die Initiierung weiterer manueller oder zeitgesteuerter Updates. Es wird damit jedoch bis zum nächsten erfolgreichen Abruf der Aktualisierungsdateien auf den Fehlerbefund hingewiesen.

10.3 Manuelles Update

Die Durchführung einer Systemaktualisierung erfordert eine Anmeldung als Administrator ***update***.

Über den Menüpunkt ***update > Auto-Update*** werden automatisch die verfügbaren Aktualisierungen vom Update-Server der m-privacy GmbH heruntergeladen und installiert. Anschließend werden alle Dienste neu gestartet. Auto-Update ist dabei nicht mit den ebenfalls möglichen, zeitgesteuerten Updates zu verwechseln. Während zeitgesteuerte Updates zu einem festgelegten Zeitpunkt von selbst anlaufen, ist bei Auto-Update nur der Aktualisierungsprozess an sich automatisch. Er muss jedoch manuell durch Aufruf des Menüpunkts ***update > Auto-Update*** angestoßen werden.

Warnungen:

- Ein Einzelsystem darf nicht mit angemeldeten Benutzern aktualisiert werden, bei einem Verbundrechnersystem (Cluster) muss der zu aktualisierende Knoten (Node) ohne angemeldete Benutzer laufen. Deshalb werden alle laufenden Benutzersitzungen nach einer Rückfrage beendet. Es kann hierbei unter Umständen auch zu Datenverlust aufseiten der Benutzer kommen. Vor einer Systemaktualisierung sollten die bevorstehenden Wartungsarbeiten über das interne Benachrichtigungssystem von TightGate®-Pro Server mit hinreichendem zeitlichen Vorlauf angekündigt werden. Benutzer erhalten so die Gelegenheit, ihre Arbeiten abzuschließen und wichtige Daten zu speichern, bevor das Update beginnt.
- Der Menüpunkt ***Kundendienst*** samt Untermenüs hat für die reguläre Softwarepflege keine Bedeutung. Einstellungen in diesem Bereich sollen nur nach Aufforderung durch den technischen Kundendienst der m-privacy GmbH vorgenommen werden. Ein entsprechender Warnhinweis weist auf diesen Sachverhalt hin. Generell empfiehlt es sich, die im Rahmen dieser Dokumentation nicht näher erläuterten Update-Optionen nur in Absprache mit dem technischen Kundendienst der m-privacy GmbH einzusetzen.

Hinweise:

- Vor jedem Aktualisierungslauf wird in jedem Fall geprüft, ob Updates auf den Update-Servern der m-privacy GmbH verfügbar sind. Ist dies nicht der Fall, wird der Vorgang abgebrochen, die angemeldeten Benutzer werden nicht abgemeldet.
- Bei Clustersystemen (Rechnerverbünden) wird empfohlen, in Absprache mit der m-privacy GmbH eine Aktualisierungsstrategie festzulegen.
- Der gesamte Aktualisierungsvorgang kann in Abhängigkeit vom Volumen der Updates und der verfügbaren Bandbreite der Internetanbindung einige Zeit dauern. TightGate®-Pro Server gibt eine Warnmeldung aus, wenn auf einer Partition der eingebauten Festplatten weniger als 20% freier Platz verfügbar ist. Es empfiehlt sich in einem solchen Fall, Kontakt mit dem technischen Kundendienst der m-privacy GmbH aufzunehmen.
- Die Aktualisierung von TightGate®-Pro Server via Socks oder unverschlüsselt über einen Proxy-Server wird nicht mehr unterstützt.

10.4 Zeitgesteuertes Update

TightGate®-Pro Server bietet die Option, den Aktualisierungsprozess ohne Eingriff zu einem bestimmten Zeitpunkt automatisch anlaufen zu lassen. Über den Menüpunkt ***update > Zeitgesteuertes Update*** können hierzu Wochentag und Uhrzeit angegeben werden.

Zwei Stunden vor dem konfigurierten Zeitpunkt nimmt TightGate®-Pro Server Kontakt zu den Aktualisierungsservern der m-privacy GmbH auf. Sind keine Updates verfügbar, wird der Prozess bis zum nächsten terminierten Aktualisierungslauf beendet und das Ergebnis protokolliert. Sind hingegen Updates verfügbar, wird der Wartungs-Betrieb aktiviert, d. h. angemeldete Benutzer erhalten einen Hinweis auf

die bevorstehende Trennung ihrer Benutzersitzung. Einzelsysteme deaktivieren die Klienten-Anmeldung unmittelbar vor Beginn des Aktualisierungsprozesses (nicht des Downloads!), bei Verbundrechnersystemen (Cluster) wird der zu aktualisierende Knoten (Node) des Rechnerverbunds von der Lastverteilung ausgenommen (eine direkte Klienten-Anmeldung bleibt bis zum eigentlichen Start der Aktualisierung weiterhin möglich).

Zum konfigurierten Zeitpunkt werden alle angemeldeten Benutzer getrennt, die Updates werden abgerufen und installiert. Abschließend erfolgt ein Neustart des Systems bzw. des Knotens, sofern infolge des Updates erforderlich. Bei durchgängig fehlerfreiem Ablauf wird der Wartungs-Betrieb aufgehoben und die VNC-Anmeldung für Benutzer wieder freigegeben. Auch diese Aktivitäten werden protokolliert.

Schlägt eine die Installation eines Updates fehl, bleibt der Wartungs-Betrieb eingeschaltet und die VNC-Anmeldung gesperrt. Der Systemadministrator kann den Sachverhalt prüfen und den Server nach Beseitigung der Ursache manuell wieder freigeben. Der fortbestehende Wartungs-Betrieb wird in der Nagios-Systemüberwachung angezeigt. Gleichzeitig wird das zeitgesteuerte Update für weitere Knoten bis zur Fehlerbeseitigung ausgesetzt, um einem sukzessiven Ausfall des gesamten Rechnerverbunds durch fehlerhafte Updates vorzubeugen.

Hinweis: Wenn ein zeitgesteuertes Update fehlschlägt, wird automatisch ein Update-Lock gesetzt, das weitere Update-Versuche zunächst unterbindet. In diesem Fall wird im Hauptmenü des Administrators ***update*** eine Menüoption ***Update-Lock entfernen*** eingeblendet. Diese muss gewählt werden, um die Sperre aufzuheben und einen erneuten Aktualisierungslauf zu ermöglichen.

Achtung: In Rechnerverbünden (Cluster-Systemen) kann immer nur ein Knoten (Node) zum gleichen Zeitpunkt zeitgesteuerte Updates durchführen. Es ist unbedingt darauf zu achten, nicht zwei Knoten eines Rechnerverbunds auf denselben Update-Zeitpunkt zu konfigurieren. Es wird empfohlen, zeitgesteuerte Updates bei komplexen Rechnerverbünden (Cluster-Systemen) nur nach Rücksprache mit dem technischen Kundendienst der m-privacy GmbH zu nutzen.

10.5 Außerplanmäßige Aktualisierungen (Hotfixes)

Besondere Situationen können in seltenen Fällen außerplanmäßige Updates bei TightGate®-Pro Server erforderlich machen. Der technische Kundendienst der m-privacy GmbH informiert Anwender in jedem Fall, in dem außerplanmäßige Aktualisierungen („Hotfixes") eingespielt werden sollten, per E-Mail und in dringenden Fällen zusätzlich telefonisch. Diese Leistungen sind in allen Softwarepflegestufen inbegriffen.

Außerplanmäßige Updates werden grundsätzlich nicht vollautomatisch installiert. Sie müssen explizit ausgewählt und manuell ausgelöst oder zeitgesteuert installiert werden. Dies erfolgt im Kundendienstmenü des Administrators ***update***.

Warnung: Verwenden Sie das Kundendienst-Menü des Administrators ***update*** nur dann, wenn Sie außerplanmäßige Aktualisierungen („Hotfixes") installieren müssen oder per E-Mail oder telefonisch durch den technischen Kundendienst der m-privacy GmbH aus anderen Gründen hierzu aufgefordert werden. Falsche Anwendung der Einstelloptionen im Kundendienstmenü kann erhebliche Funktionsstörungen oder den Ausfall von TightGate®-Pro Server zur Folge haben. Eine zusätzliche Sicherheitsabfrage weist bei jedem Aufruf des Kundendienstmenüs nochmals auf diesen Zusammenhang hin.

10.5.1 Hotfixes planen

Bevor außerplanmäßige Aktualisierungen eingespielt werden können, müssen sie zunächst zur Installation vorgesehen werden. Dies geschieht unter ***update > Kundendienst > Hotfixes*** **aus Prestable planen**. Nach kurzer Wartezeit wird eine Liste der verfügbaren Hotfixes angezeigt. Es dürfen nur solche Pakete ausgewählt werden, die vom technischen Kundendienst der m-privacy GmbH in der Vorabinformation aufgeführt sind.

Warnung: Die Installation anderer Pakete kann schwere Funktionsstörungen bei TightGate®-Pro Server verursachen!

Hinweis: Bei Bedarf können verfügbare Aktualisierungen über die Option ***update > Kundendienst > Download Prestable*** im Vorfeld des Installationszeitpunktes vorab heruntergeladen werden. Dies verkürzt insbesondere bei langsamer Verbindung zum Update-Server den Zeitbedarf für den eigentlichen Aktualisierungslauf. Installiert werden jedoch nur die Updates, die explizit ausgewählt wurden.

10.5.2 Hotfixes installieren

Nach der Auswahl können außerplanmäßige Updates entweder manuell über die Option ***update > Auto-Update*** oder ***update > Zeitgesteuertes Update*** installiert werden. In den meisten Fällen ist ein manuelles Update empfehlenswert, um eventuelle Probleme sofort zu erkennen.

10.6 Updates bei TightGate®-Pro (CC) Version 1.4 Server

TightGate®-Pro (CC) Version 1.4 Server kann ebenfalls über die integrierte Update-Funktion aktualisiert werden. Dabei kann jedoch die CC-Konformität beeinträchtigt oder aufgehoben werden. Daher ist es notwendig, dass der Update-Status von TightGate®-Pro (CC) Version 1.4 Server jederzeit erkennbar ist. Wurden Updates eingespielt, erscheint in der Titelzeile der gelb dargestellte Hinweis „+Updates“. Ein weiterer Hinweis bei dem jeweiligen Menüpunkt stellt Abweichung und Vorgabe gegenüber. Der Hintergrund des Menübildschirms wechselt bei Abweichungen von CC-konformen Vorgaben von Blau nach Gelb, solange diese Abweichungen bestehen.

10.7 Landesspezifische Schriftzeichen über IBus

Mehrsprachigkeit bei der Eingabe landesspezifischer Sonderzeichen wird in TightGate®-Pro Server mittels des Frameworks „IBus“ (Intelligent Input Bus) realisiert. IBus kann als Administrator ***update*** eingerichtet und dann als angemeldeter VNC-Benutzer in allen Eingabemasken des Systems und im Webbrowser verwendet werden. Zu diesem Zweck sind zunächst als Administrator ***update*** die IBus-Module auszuwählen, für die Unterstützung bei der Eingabe landesspezifischer Schriftzeichen gewünscht wird. Nach einer kurzen Wartezeit stehen die installierten IBus-Module dann allen angemeldeten VNC-Benutzern zur Verfügung.

10.7.1 Auswahl benötigter IBus-Module

Die Sprachunterstützung via IBus gliedert sich in Module für unterschiedliche Sprachen. Diese sind zunächst als Administrator ***update*** zu installieren:

- Nach der Anmeldung als Administrator *update* können die gewünschten Sprachmodule unter ***update > IBus-Module hinzufügen*** ausgewählt und installiert werden.
- Die installierten Module stehen nach kurzer Wartezeit allen VNC-Benutzern zur Verfügung, in deren LXDE-Optionen das iBus-Verfahren konfiguriert wurde..

10.7.2 Nutzung des IBus-Eingabeverfahrens

Nach der Installation der gewünschten IBus-Sprachmodule kann die IBus-Eingabemethode von angemeldeten VNC-Benutzern verwendet werden, um landesspezifische Schriftzeichen fremder Sprachen einzugeben. IBus wirkt dabei auf alle Eingabemasken des Systems, also insbesondere auch auf die Adresszeile des Webbrowsers oder Eingabefelder in Masken und Formularen. Bevor mit der Eingabe landesspezifischer Sonderzeichen via IBus begonnen werden kann, muss IBus in den LXDE-Optionen des jeweiligen Benutzerkontos freigegeben sein. Es erscheint ein Icon in der Startleiste (Tray) als Anzeige, dass das IBus-Framework gestartet wurde.

Danach ist das Sprachmodul auszuwählen, aus dem Sonderzeichen eingegeben werden sollen:

Nach Anmeldung als VNC-Benutzer muss zunächst das IBus-Framework unter ***Startmenü des Benutzers > Einstellungen > IBus-Einstellungen*** gestartet werden. Die gestellte Sicherheitsabfrage ist mit „Ja“ zu bestätigen.

Es öffnet sich ein Dialogfeld mit Einstelloptionen. In Reiter ***Eingabemethode*** müssen nun die installierten IBus-Module der Liste zu verwendender IBus-Module zugefügt werden. Dies geschieht über die

Schaltflächen ***Eingabemethode wählen*** und ***Hinzufügen***. Nicht mehr benötigte Module können der Übersicht halber mit der Schaltfläche ***Entfernen*** aus der Liste zu verwendender Module entfernt werden. Die Liste der zu verwendenden IBus-Module kann zudem hinsichtlich der Abfolge der Einträge sortiert werden. Alle Einstellungen werden dauerhaft gespeichert und erleichtern den Zugriff auf die IBus-Module während der Eingabe landesspezifischer Sonderzeichen.

Zur Eingabe landesspezifischer Sonderzeichen muss zunächst der Fokus auf einem Eingabefeld liegen (Mauszeiger im Eingabefeld platzieren und einmal klicken). Blinkt die Schreibmarke (Cursor) im Eingabefeld, kann durch Klick auf das Tray-Icon aus dem sich öffnenden Kontextmenü ein IBus-Modul aus der zuvor festgelegten Liste der zu verwendenden IBus-Module ausgewählt werden.

Anschließend können landesspezifische Sonderzeichen im Eingabefeld eingegeben werden. Ein Kontextmenü bietet je nach vorgegebenem Buchstaben sinnvolle Optionen landesspezifischer Sonderzeichen an, die übernommen werden können.

Hinweis: Der IBus-Modus bleibt so lange eingeschaltet, bis dieser über das Tray-Icon wieder verlassen wird (Mausklick auf das Tray-Icon mit der linken Maustaste und Auswahl von ***Eingabemethode ausschalten***).

10.8 Integritätsprüfung (intern / extern)

TightGate®-Pro Server kann auf Systemintegrität geprüft werden, um eine mögliche Kompromittierung der Programmkomponenten respektive Pakete zu erkennen und geeignete Gegenmaßnahmen einzuleiten. Es wird zwischen interner und externer Integritätsprüfung unterschieden.

10.8.1 Genereller Ablauf

Jedes in einem TG-Pro-System installierte Paket enthält MD5- und SHA256-Hashwerte für diejenigen darin enthaltenen Dateien, die im System nicht verändert werden dürfen. Die Tabelle mit den Hash-Werten ist herstellerseitig mit GnuPG signiert.

Die Integritätsprüfung durchläuft die Liste aller installierten Pakete, prüft zunächst die Signatur der MD5-Hashtabelle anhand des zur Signatur verwendeten Public Keys und anschließend die MD5-Hashwerte aller dort gelisteten Dateien. Jede Abweichung wird im Protokoll mit Paket- und Dateiname festgehalten.

Der Administrator ***update*** verfügt hierzu über die gesonderte Menüoption ***Integritätsprüfung***, über die eine interne Integritätsprüfung im laufenden Systembetrieb veranlasst werden kann. Weiterhin besteht die Möglichkeit, nach dem Systemstart von einem Installationsmedium die Menüoption ***tightgate-install > Integrity Check*** auszuwählen.

Der Unterschied zwischen der Prüfung als Administrator ***update*** im laufenden System und vom Installations- und Rettungs-System im Vorfeld eines sogenannten OE.Resets besteht nicht im Algorithmus, sondern nur darin, wo verwendete Programme und der Public-Key gespeichert sind. Im Fall der internen Integritätsprüfung durch den Administrator ***update*** befinden diese sich auf der Festplatte des zu prüfenden Systems und könnten prinzipiell manipuliert worden sein, während beim Aufruf vom Rettungssystem bzw. einem Installationsdatenträger im Vorfeld eines OE.Resets alle Programme und Public Keys ausschließlich vom nur lesbaren Medium geladen werden. Die signierten Hashtabellen befinden sich dagegen immer auf der Festplatte. Dies stellt kein Sicherheitsrisiko dar, da die Signaturprüfung deren Manipulation zuverlässig ausschließt.

10.8.2 Maßnahmen bei Abweichungen im Zuge der Integritätsprüfung

Sollte die Integritätsprüfung eine Veränderung entdecken, ist die Protokolldatei per E-Mail oder SCP auf ein anderes System zu übertragen und zwecks weiterer Untersuchung an den Hersteller (m-privacy GmbH) zu übermitteln. Anschließend muss das System durch eine Neuinstallation (OE-Reset) in den Auslieferungszustand zurückgesetzt werden. Die Konfiguration, die Benutzerkonten und ihre Daten sind danach wie vorgesehen zurückzuspielen. Dadurch wird sichergestellt, dass eventuelle Manipula-

tionen an den Dateien beseitigt sind. Bei Verdacht auf einen Fehlalarm empfiehlt es sich, die Integritätsprüfung erneut durchzuführen.

Hinweis: In CC-konformen Umgebungen ist eine externe Integritätsprüfung von TightGate®-Pro (CC) Version 1.4 Server gegen die Daten eines externen, unveränderlichen Datenträgers in regelmäßigen Abständen vorzusehen.

10.8.3 Verfahrensweise zur internen Integritätsprüfung

Die interne Integritätsprüfung prüft die installierten Pakete von TightGate®-Pro Server im laufenden Systembetrieb auf Integrität. Die Prüfung wird durch den Administrator ***update*** ausgelöst und umfasst die folgenden Schritte:

1. Anmeldung als Administrator ***update*** an der Konsole.
2. Auswahl der Menüoption ***update > Integritätsprüfung***.

Die Integritätsprüfung wird gestartet. Der Prozess kann je nach Systemleistung und Anzahl der zu überprüfenden Programmpakete einige Zeit in Anspruch nehmen. Mittels der Tastenkombination ***CTRL+C*** beziehungsweise ***STRG+C*** kann die Integritätsprüfung unterbrochen werden. Es wird ein Hilfsmenü angezeigt, womit die Prüfungsergebnisse angezeigt, per SCP übertragen oder per E-Mail versandt werden können. Auch der definitive Abbruch der Integritätsprüfung ist möglich.

Das Ergebnis der Integritätsprüfung wird durch eine Ergebnismeldung zusammengefasst und in einer detaillierten Protokolldatei gespeichert. Ergebnismeldungen lauten beispielhaft:

- Positiv: „All 1265 packages passed!“
- Negativ: „2 of 1265 packages failed. Please contact m-privacy support.“

Die Zahl der zu prüfenden Pakete kann abweichen und hängt von der tatsächlichen Systemkonfiguration ab. Die detaillierte Protokolldatei kann mittels der Menüoption ***Bildschirm*** angezeigt oder per E-Mail versandt werden.

Achtung: Wird die Funktion vorzeitig abgebrochen, kann der ausgegebene Ergebnisbericht fehlerhaft oder unvollständig sein.

Warnung: Die interne Integritätsprüfung ist zur Wahrung der Integrität für TightGate®-Pro (CC) Version 1.4 Server nicht ausreichend! In CC-konformen Umgebungen ist eine regelmäßige externe Integritätsprüfung von TightGate®-Pro (CC) Version 1.4 Server gegen die Daten eines externen, unveränderlichen Datenträgers in regelmäßigen Abständen obligatorisch.

10.8.4 Verfahrensweise zur externen Integritätsprüfung

Die externe Integritätsprüfung prüft die installierten Pakete von TightGate®-Pro Server gegen die Daten eines externen, unveränderlichen Datenträgers. Dabei kann es sich um ein Rettungssystem oder die im Lieferumfang von TightGate®-Pro (CC) Version 1.4 Server befindlichen Installationsmedien handeln.
Die Prüfung wird nach dem Systemstart (Bootvorgang) vom externen Datenträger durch Wahl der entsprechenden Menüoption ausgelöst und umfasst die folgenden Schritte:

1. Systemstart (Bootvorgang) vom Rettungssystem oder Installationsdatenträger.
2. Auswahl der Menüoption ***tightgate-install > Integrity Check***
3. Einhängen der Festplatte(n) des Systems in den Verzeichnisbaum: /dev/sda1 ist die Root-Partition, Rest entsprechend Vorgabe.
4. Auslösung des Prüfvorgangs.
5. Auswertung des Ergebnisses mit der Menüoption ***Screen*** beziehungsweise Versand des Prüfergebnisses per E-Mail.

Die Integritätsprüfung wird gestartet. Der Prozess kann je nach Systemleistung und Anzahl der zu überprüfenden Programmpakete einige Zeit in Anspruch nehmen. Mittels der Tastenkombination ***CTRL+C*** beziehungsweise ***STRG+C*** kann die Integritätsprüfung unterbrochen werden. Es wird ein Hilfsmenü an-

gezeigt, womit die Prüfungsergebnisse angezeigt oder per E-Mail oder SCP versandt werden können. Auch der definitive Abbruch der Integritätsprüfung ist möglich.

Das Ergebnis der Integritätsprüfung wird durch eine Ergebnismeldung zusammengefasst und in einer temporären Protokolldatei im Verzeichnis /tmp des laufenden Systems gespeichert. Ergebnismeldungen lauten beispielhaft:

- Positiv: „All 1265 packages passed!“
- Negativ: „2 of 1265 packages failed. Please contact m-privacy support.“

Die Zahl der zu prüfenden Pakete kann abweichen und hängt von der tatsächlichen Systemkonfiguration ab. Die temporäre Protokolldatei kann mittels der Menüoption ***Screen*** angezeigt sowie ausschließlich über die jeweiligen Menüoptionen per SCP übertragen oder per E-Mail versandt werden, sofern dies in der Einsatzumgebung vorgesehen ist.

Achtung: Wird die Funktion vorzeitig abgebrochen, kann der ausgegebene Ergebnisbericht fehlerhaft oder unvollständig sein.

Hinweis: In CC-konformen Umgebungen ist eine regelmäßige externe Integritätsprüfung von TightGate®-Pro (CC) Version 1.4 Server gegen die Daten eines externen, unveränderlichen Datenträgers in regelmäßigen Abständen vorgesehen. Bei Beanstandungen im Zuge des Prüfprozesses sollte in jedem Fall Kontakt zur m-privacy GmbH aufgenommen werden.

11 Drucker einrichten

Über TightGate®-Pro kann auf drei Arten gedruckt werden:

- Drucken über einen bestehenden CUPS-Druckserver
- Drucken über das Betriebssystem des Klientenrechners mittels des Druckspoolers von TightGate®-Pro Server

Hinweis: Vor jeder Druckausgabe wird dem Benutzer ein Dialogfenster angezeigt, welches die Wahl zwischen der Ausgabe auf einem physikalischen Drucker und der Ablage als PDF-Datei ermöglicht. Der Druckdialog verzweigt anschließend je nach gewähltem Ausgabemedium. Generierte PDF-Dateien werden automatisch im Verzeichnis ***transfer*** (Schleusenverzeichnis) abgelegt.

Die Druckausgabe über einen lokalen, in TightGate®-Pro Server integrierten CUPS-Druckserver wird ab Build 1.4-780 nicht mehr unterstützt. Es wird empfohlen, den integrierten Druckspooler zu verwenden, zumal die verfügbaren Klientenprogramme diese Option unterstützen.

11.1 Drucken über einen externen CUPS-Druckserver

TightGate®-Pro Server kann auf einen bestehenden CUPS-Druckserver zugreifen. Dieses Vorgehen empfiehlt sich besonders bei Cluster-Systemen, um die mehrfache Einrichtung der Drucker zu vermeiden.

Die folgenden Konfigurationsoptionen sind nach Anmeldung als Administrator ***config*** zugänglich:

config > Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
CUPS-Druckserver-IP	IPv4-Adresse des externen CUPS-Druckservers im Netzwerk.		**E5**	**F5**
CUPS-Druckserver-Name	Druckserver-Name zur Namensauflösung (inkl. Domäne, optional).		**E4**	
CUPS kurze Namen	Einstellung des Druckdienstes CUPS (optional). Der an dieser Stelle angegebene Parameter muss mit dem im CUPS-Druckserver hinterlegten Wert übereinstimmen.		**E1**	

Hinweis: Nach den Änderungen als Administrator ***config*** sind diese durch ***Speichern*** und ***Sanft Anwenden*** zu aktivieren.

11.2 Drucken über den integrierten CUPS-Druckserver

Die Druckausgabe über einen lokalen, in TightGate®-Pro Server integrierten CUPS-Druckserver wird ab Build 1.4-780 nicht mehr unterstützt. Es wird empfohlen, den integrierten Druckspooler zu verwenden, zumal die verfügbaren Klientenprogramme diese Option unterstützen.

11.3 Drucken über den integrierten Druckspooler

TightGate®-Pro Server verfügt über einen integrierten Druckspooler, der als Administrator ***config*** global für alle neu anzulegenden Benutzerkonten vorgegeben werden kann. Der Druckspooler kann auch nachträglich nutzerindividuell oder gruppenbezogen als Administrator ***maint*** zu- respektive abgeschaltet werden.

Achtung: Damit der Druckspooler funktioniert, muss die Dateischleuse durch den Administrator ***config*** global erlaubt sein, weiterhin muss jeder Benutzer durch den Administrator ***maint*** oder per Vorgabe beim Anlegen des Benutzerkontos die allgemeine Schleusenberechtigung erhalten. Welche Dateitypen für die Schleuse zugelassen sind, ist für die Funktion des Druckspoolers irrelevant. Ist jedoch die

Dateischleuse global deaktiviert, kann kein Benutzer den auf TightGate®-Pro Server integrierten Druckspooler nutzen. Verfügt ein Benutzer nicht über eine allgemeine Schleusenberechtigung, ist diesem Benutzer die Verwendung des Druckspoolers nicht möglich.

Wird der Druckspooler aktiviert, generiert TightGate®-Pro Server aus jedem Druckauftrag, der im Auswahldialog an den „Drucker“ gesandt wird, eine PDF-Datei und legt diese im Pufferverzeichnis .spool im Dateibereich des Benutzers ab. Eine Hilfsapplikation auf dem Klientenrechner prüft regelmäßig, ob Druckaufträge vorliegen, überträgt diese verschlüsselt auf die Arbeitsplatzstation und leitet sie automatisch dem Drucksystem des dort installierten Betriebssystems zu.

Dieses Verfahren hat den Vorteil, dass keine weiteren Druckdienste oder Printserver erforderlich sind. Der Benutzer kann die gewohnte Umgebung der bestehenden Infrastruktur nutzen, um Dokumente auf beliebige Drucker im internen Netzwerk auszugeben. Die gesamte Geräteverwaltung (Anschluss, Treiberunterstützung) erfolgt in diesem Fall nicht über TightGate®-Pro Server, sondern über das interne Netzwerk und die darin befindlichen Ressourcen.

Zur Nutzung des in TightGate®-Pro Server integrierten Druckspoolers ist eine Hilfsapplikation erforderlich, die im Download-Bereich der Internetpräsenz der m-privacy GmbH lizenzkostenfrei erhältlich ist. Diese Hilfsapplikation ist auf allen Klientenrechnern zu installieren, die den Druckspooler von TightGate®-Pro Server nutzen sollen. Sie wird zusammen mit der Viewer-Applikation (TightGate®-Pro Client) gestartet und prüft das Verzeichnis .spool auf TightGate®-Pro Server im Hintergrund auf neue Druckaufträge.

Das Klientenseitige Abholintervall für Druckaufträge kann als Administrator ***config*** unter ***Einstellungen > Drucken in Spool: Intervall*** festgelegt werden.

Hinweis: Der TightGate®-Druckspooler kann nur verwendet werden, wenn die Authentisierung der Klienten an TightGate®-Pro Server per Single Sign-on (SSO) erfolgt; entweder über serverseitig erzeugte Zertifikate oder über ein Active Directory (AD).

Soll wieder eine der anderen Verfahrensweisen zur Druckausgabe aus TightGate®-Pro Server genutzt werden, ist die entsprechende Option als Administrator ***maint*** für die betreffenden Benutzer abzuschalten und die Hilfsapplikation von deren Arbeitsplatzrechnern zu deinstallieren.

11.4 Speicherung des Bildschirminhalts (Screenshot)

Der Bildschirminhalt, der mittels der Viewer-Applikation TightGate®-Pro Client angezeigt wird, kann jederzeit über die „Drucken“-Taste am Klientenrechner „eingefroren“ und gespeichert werden, sofern der Maus-Fokus in diesem Moment auf dem Viewer-Fenster lag. Es öffnet sich ein Dialogfenster, womit sich der Bildschirminhalt speichern lässt. Als Zielverzeichnis muss das transfer-Verzeichnis manuell ausgewählt werden. Eine entsprechende Vorgabe des Dateipfads ist technisch nicht möglich. Die Datei kann nicht in ein anderes Verzeichnis gespeichert werden, in diesem Fall erfolgt eine Fehlermeldung.

12 Benutzerrolle “Revision“

Die Rolle des Revisors/Datenschutzbeauftragten wurde im Zuge der organisatorischen Trennung von technischer und inhaltlicher Kontrolle eingeführt. Während die technische Kontrolle von Systemadministrator-Rollen durchgeführt wird, haben diese keinen Zugriff auf Benutzerdaten. Die inhaltliche Kontrolle der Benutzerdaten kann nur durch die Rolle ***revision*** erfolgen.

Gesetzliche Vorgaben, darunter insbesondere Datenschutzvorschriften, setzen enge Grenzen. Besonders der Revisor bzw. Datenschutzbeauftragte ist angehalten, verantwortungsvoll und unter Abwägung aller Umstände zu entscheiden, ob und wie eine Kontrolle der Benutzerdaten erforderlich ist. Die Rolle ***revision*** ist auf die Bedürfnisse und Aufgabenstellungen der Datenschutzbeauftragten und Revisoren zugeschnitten.

Hinweis:
revision ist ein Benutzer, d. h. der Zugang erfolgt nicht über die Konsole, sondern über die Viewer-Software an TightGate®-Pro Server. Der Revisionsaccount ist jedoch kein Benutzerkonto im herkömmlichen Sinne, vielmehr dient die Verwendung dieses Accounts ausschließlich der Wahrnehmung von Kontrollrechten im Rahmen der Aufgaben eines Datenschutzbeauftragten bzw. Revisors. Dieser Zugang ersetzt nicht das normale Benutzerkonto für mit Datenschutz- bzw. Revisionsaufgaben betraute Mitarbeiter. Es besteht insbesondere keine Möglichkeit, E-Mail-, Internet- oder andere Netzwerk-Dienste zu nutzen.

12.1 Funktion und Grenzen der Revisor-Rolle

12.1.1 Funktion

1. Es besteht die Möglichkeit, als ***revision*** sämtliche Benutzerdaten (jeweils eines Benutzerkontos) in den Bereich des Revisionsaccounts zu kopieren und dort mit den Einstellungen des betreffenden Benutzers zu kontrollieren.
2. Es sollten aus Platzgründen jeweils nur die Daten eines Benutzers kopiert und gesichtet werden, das System unterstützt aber mehrere gleichzeitige Kopien.
3. Zur Sichtung stehen dieselben Programme zur Verfügung, mit denen die Daten vom Benutzer bearbeitet werden.
4. Es können Daten in der Revisionskopie gespeichert werden, nicht jedoch im ursprünglichen Benutzerverzeichnis.
5. Hat ein Benutzer ein Programm bisher nicht verwendet, liegt u. U. keine entsprechende Konfiguration vor und es werden möglicherweise Fehlermeldungen angezeigt.

12.1.2 Beschränkungen

1. Der ***revision***-Zugang hat ein ausschließlich lesendes Zugriffsrecht auf die Benutzerdaten, um eine (Sicherungs-)Kopie zur Analyse zu erstellen. Somit können durch den Benutzer ***revision*** keine veränderten Daten in Benutzerkonten zurückgeschrieben werden.
2. Gleiches gilt für alle Einstellungen im Benutzeraccount. Eventuell durch den Administrator ***revision*** veränderte Einstellungen können nicht auf den Benutzeraccount übertragen werden.
3. Der Benutzer ***revision*** kann, trotz Übernahme sämtlicher Benutzereinstellungen, keine E-Mails aus dem kopierten Benutzer-Account verschicken; weder im eigenen Namen, noch im Namen des Benutzers.
4. IMAP-Mailkonten können auf TightGate®-Pro Server nicht kontrolliert werden. Es handelt sich dabei um Postfächer auf einem entfernten Mailserver. Eine Kontrolle dieser Postfächer ist nur dort möglich.

12.2 Benutzerkontrolle durch den Revisor

Der Benutzer ***revision*** ist eine speziell für den Datenschutzbeauftragten geschaffene Rolle. Um den Status des Revisors zu erlangen, ist die Anmeldung mit dem Benutzernamen ***revision*** und dem zugehörigen Passwort erforderlich. Das Passwort für den Benutzer ***revision*** wird vom Administrator ***security*** vergeben. Die Anmeldung erfolgt, analog zur Anmeldung anderer Benutzer, über die grafische Viewer-Software.

Es erscheint ein zusätzliches Programm, das ***Revisionsmenü,*** auf der Arbeitsoberfläche. Ansonsten gleicht die Arbeitsoberfläche der von normalen Benutzern. Zur Warnung ist der Bildschirmhintergrund leuchtend rot.

revision > Revisionsmenü (grafische Benutzeroberfläche nach Login über Viewer)		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Kopieren	Nach Auswahl einer Benutzerkennung in der Spalte „Benutzername“ werden die Daten durch diese Schaltfläche einer Sichtung durch den Benutzer ***revision*** zugänglich. Es wird eine lokale Kopie der betreffenden Benutzerdaten angelegt. **Hinweis:** Die Kopie der Benutzerdaten kann auch verändert bzw. in veränderter Form gespeichert werden. Die originären Benutzerdaten werden dabei zu keinem Zeitpunkt angetastet.		**E0**	
Löschen	Löscht die Arbeitskopie eines Benutzerdatensatzes aus dem Arbeitsbereich des Benutzers ***revision***.		**E0**	
Dateien ansehen	Öffnet einen Dateibrowser zur Sichtung der Dateien des ausgewählten Benutzers, dessen Daten zuvor in den Arbeitsbereich des Benutzers ***revision*** kopiert wurden.		**E0**	
Firefox / Iceweasel	Startet den Webbrowser exakt mit denselben Voreinstellungen eines Benutzers. Dessen Daten müssen zu diesem Zweck zunächst in den Arbeitsbereich des Benutzers ***revision*** kopiert werden (siehe oben). **Hinweis:** Hat der ausgewählte Benutzer den betreffenden Web-Browser noch nicht verwendet, liegt u. U. keine entsprechende Konfiguration vor und es werden möglicherweise Fehlermeldungen angezeigt.		**E0**	
Thunderbird / Icedove	Startet das E-Mail-Programm exakt mit denselben Voreinstellungen eines Benutzers. Dessen Daten müssen zu diesem Zweck zunächst in den Arbeitsbereich des Benutzers ***revision*** kopiert werden (siehe oben). **Hinweis:** Es können die E-Mails des jeweiligen Benutzers eingesehen werden. E-Mail-Versand ist nicht möglich. Hat der ausgewählte Benutzer das betreffende E-Mail-Programm noch nicht nicht verwendet, liegt u. U. keine entsprechende Konfiguration vor und es werden möglicherweise Fehlermeldungen angezeigt.		**E0**	
Benutzer-Proxy-Proto	Zeigt die Logdatei des Proxy-Speichers an und erlaubt die Kontrolle aufgerufener Seiten im WWW durch den betreffenden Benutzer.		**E0**	
Pseudonym auflösen	Nach Eingabe eines aufzulösenden Pseudonym wird die jeweilige Benutzerkennung im Klartext angezeigt.		**E0**	
Generiere Proxy-Report	Erstellt eine zusammenfassende Auswertung der gespeicherten Proxy-Protokolle, siehe ***config***-Einstellung „Proxy-Protokoll“. **Hinweis**: Es stehen nur Protokoll-Daten bis zum Vortag bereit.		**E0**	

revision > Revisionsmenü (grafische Benutzeroberfläche nach Login über Viewer)		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Zeige Proxy-Report	Zeigt die Auswertung der Proxy-Protokolle, die zuvor erstellt werden müssen (siehe oben).		**E0**	
Ende	Schließen des Revisionsmenüs. Der Benutzer ***revision*** bleibt jedoch an TightGate®-Pro Server angemeldet. Das Revisionsmenü kann über die entsprechende Schaltfläche auf dem Desktop des Benutzers ***revision*** erneut aufgerufen werden.		**E0**	

12.2.1 Benutzer überprüfen über Protokolle

Der Benutzer ***revision*** kann die Arbeitsumgebung inklusive aller Daten eines Benutzers kopieren, um sie anschließend einer Prüfung zu unterziehen. Um die Daten eines Benutzers zu kopieren, wird die betreffende Benutzerkennung aus einer Liste ausgewählt und dann über die Funktion ***Kopieren*** des Revisionsmenüs eine lokale Kopie des Benutzerverzeichnisses im Arbeitsbereich des Benutzers ***revision*** angelegt.

Weiterhin kann der Benutzer ***revision*** diverse Systemprotokolle sichten. Diese werden nur nach Freigabe durch den Administrator ***config*** wahlweise mit Benutzerkennung im Klartext, mit Pseudonym oder ohne Kennung (anonym) geschrieben. Die Protokollierung lässt sich unter ***config > Einstellungen > Proxy-Protokoll*** aktivieren. Unter ***config > Einstellungen > Pseudonymisierung*** kann die Pseudonymisierung eingeschaltet werden. Es werden dann statt der Benutzerkennungen im Klartext Pseudonyme verwendet, die im Bedarfsfall durch den Benutzer ***revision*** rückaufgelöst werden können.

Damit die Protokolle dem Benutzer ***revision*** zur Auswertung zur Verfügung stehen, muss unter ***config > Einstellungen > Proxy-Protokoll-Lebensdauer*** unbedingt eine Protokollierungsfrist hinterlegt werden. Nur Proxy-Protokolle aus diesem Zeitraum stehen dem Benutzer ***revision*** zur Auswertung zur Verfügung.

Achtung: Wird keine Protokollierungsfrist angegeben, werden zwar Protokolle geschrieben, diese stehen jedoch dem Benutzer ***revision*** nicht zur Verfügung.

Zur Auswertung der Internetzugriffe einzelner Benutzer steht das ***Proxy-Protokoll*** zur Verfügung. Es können zeitlich begrenzte Auszüge oder die gesamte Datei angezeigt werden. Die Datei über Benutzeranmeldungen wird als Textdatei ausgegeben und hat folgenden beispielhaften Aufbau:

Monat	Tag	Zeit	Server-Name	Protokoll	Authentifikation	Benutzer
Jan	31	12:44:53	tgpro-12	riv:	(pam_rsbac_de)	session opened for user revision by *unknown*(uid=0)
Januar	31	12:44:53	tgpro-12	riv (per VNC)	pam	revision

12.2.2 Weitere Protokolle

Auf dem Desktop des Benutzers ***revision*** befindet sich eine Schaltfläche Systemprotokolle, mit der unterschiedliche Logdateien komfortabel gesichtet werden können. Nachfolgende Tabelle führt nur die wichtigsten Logdateien auf, die durch den Benutzer ***revision*** eingesehen werden können. Unterstützung im Zusammenhang mit den Funktionen der Systemprotokollierung leistet der technische Kundendienst der m-privacy GmbH.

Protokoll	Beschreibung
auth log	Protokollierung der Authorisierungsvorgänge, Anmeldung von Benutzern und Diensten am System.
kernel log	Protokollierung der Meldungen, die vom Linux-Kern erstellt werden - insbesondere die RSBAC Fehlermeldungen.
syslog	Protokollierung der Systemdienste Proxy, cron und weitere.
daemons log	Protokollierung der Systemdienste NTP, DNS und weitere.

12.2.3 Pseudonyme in Log-Dateien auflösen

In den RSBAC-Logdateien können die Benutzernamen pseudonymisiert abgelegt werden. Auch die Anzeige der Logs erfolgt mit pseudonymisierten Benutzernamen, wenn dies eingestellt wurde. Die Auflösung der Pseudonyme ist nur manuell durch den Benutzer ***revision*** möglich.

Wurde ein Pseudonym aufgelöst und ist die Vergabe eines neuen Pseudonyms für einen Benutzer nötig, so kann der Benutzer ***security*** einzelnen Benutzern neue Pseudonyme vergeben. Es empfiehlt sich in diesem Fall die Kontaktaufnahme zum technischen Kundendienst der m-privacy GmbH. Sollen für alle Benutzer neue Pseudonyme vergeben werden, so kann der Administrator ***config*** dies durch einmaliges Aus- und erneutes Einschalten der Pseudonymisierung bewerkstelligen.

Wird ein Pseudonym geändert, so wird die Liste der alten Pseudonyme in das Verzeichnis /home/revision/pseudos gesichert und bleibt damit für die Auswertung älterer Logdateien verfügbar.

12.2.4 Speicherdauer von Log-Dateien

Reguläre Log-Dateien: Die Speicherdauer der Logdateien in TightGate®-Pro Server ist begrenzt. TightGate®-Pro Server verwendet standardmäßig einen Ringpuffer (Logrotate) für alle Logdateien. Dabei beträgt die Rotationsdauer eine Woche bei vier Zyklen. Logdateien werden vier Wochen gespeichert. Bei Erstellung der Dateien der fünften Woche werden die Daten der ersten Woche gelöscht.

Sonderfall RSBAC-Log-Dateien: Für RSBAC-Logdateien gilt ein kürzerer Zyklus. Logdateien werden sieben Tage rotierend gespeichert. Am 8. Tag wird die Logdatei des ersten Tages gelöscht.

Hinweis: Die Datei “debug.log” kann auch ältere RSBAC-Meldungen enthalten, als es gemäß der zyklischen Löschung zu erwarten wäre.

Übersicht der Logdateien, in denen RSBAC-Meldungen gespeichert sind:

kern.log
messages
syslog
debug.log (standardmäßig nicht aktiv)

13 Die Administratoren 'root' und 'security'

Die Administratoren ***root*** und ***security*** sind für die Verwaltung des Sicherheitssystems des TightGate®-Pro zuständig. Sie können Änderungen an den Sicherheitsmodellen vornehmen oder Protokollauswertungen für die Wartung bereitstellen. Für den normalen Betrieb und die Konfiguration von TightGate®-Pro Server werden sie indessen nicht benötigt.

Hinweis: In TightGate®-Pro (CC) Version 1.4 Server für CC-konforme Umgebungen sind die Administrationsrollen ***root*** und ***security*** nur verfügbar, wenn das System im Softmode gestartet wird. Die Anmeldung der Administratoren ***root*** und ***security*** per SSH ist nur dann möglich, wenn der Server im sogenannten Softmode gestartet wurde und eine IPv4-Adresse eines verwaltungsberechtigten Rechners außerhalb des Klientennetzes (!) unter ***config > Einstellungen > Wartung und Updates > Nagios / Storage IP*** hinterlegt wurde.

Warnung: Unsachgemäße Änderungen am Sicherheitssystem von TightGate®-Pro Server bergen erhebliche Sicherheitsrisiken für das interne Netzwerk und die darin befindlichen Arbeitsplatzrechner. Weiterhin können schwerwiegende Störungen des Produktivbetriebs auftreten.

Warnung: Kundendiensteinsätze der m-privacy GmbH, die vor dem Hintergrund unsachgemäßer Eingriffe über die Administratoren ***root*** und ***security*** notwendig werden, sind nicht im Rahmen der Verträge zur Softwarepflege abgedeckt. Dies gilt insbesondere auch für eventuelle Folgeschäden beispielsweise durch unzureichende Schutzwirkung infolge einer Beeinträchtigung der Sicherheitsmechanismen von TightGate®-Pro Server.

13.1 Der Administrator *security*

Die Rolle ***security*** definiert die Möglichkeiten eines Sicherheitsbeauftragten und kann das gesamte RSBAC-Regelwerk bearbeiten. Es können neue Rollen definiert und Rechte bestehender Rollen geändert werden. Aufgrund des Kompetenzumfangs ist die Rolle ***security*** in der Voreinstellung nur von der lokalen Konsole aus zugänglich. Ein SSH-Zugang für den Administrator ***security*** kann nur durch den Administrator ***maint*** für einen begrenzten Zeitraum aktiviert werden. Um den Status der Sicherheitsmodelle und das RSBAC-Regelwerk einzusehen, ist eine Anmeldung als Administrator ***security*** an der Konsole erforderlich.

Es bestehen folgende Einstellmöglichkeiten:

security		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Ende	Beenden des Zugangs als Administrator ***security***		**E2**	
Modul-Zustand	Anzeige des Status der Sicherheitsmodule. **Warnung:** Stati im Produktivbetrieb müssen sein: Mode: „secure“ Softmode / Ind-Soft: „unavailable“ Switching on / off: „unavailable“ Module (alle!): „on“ Andernfalls können weitreichende Sicherheitsdefizite die Folge sein. Zudem besteht die Gefahr erheblicher Betriebsstörungen.		**E0**	
Erlaube 5 Min. root-Wartung	Freigabe der Wartungsrolle für den Administrator ***root*** für 5 Minuten.		**E0**	
root-Wartungskonsole sperren	Dem Administrator ***root*** den Zugang zur Wartungsrolle sofort entziehen.		**E0**	
root-Wartung an	Einer Shell-Konsole des Administrators ***root*** die Berechtigungen der Wartungsrolle erteilen.		**E0**	

security		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Menü-Protokollierung an	Einschalten der Menüprotokollierung, d. h. alle Kommandos, die der Administrator ***security*** ausführt, werden im Verzeichnis /security/log/ protokolliert. Aktivitäten anderer Administrationsrollen werden nicht protokolliert.		**E0**	
Menü-Protokollierung aus	Abschalten der Menüprotokollierung.		**E0**	
Zeige Menü-Protokoll	Anzeige des Menüprotokolls.		**E0**	
Menü-Protokoll kopieren	Kopie der Menü-Protokollierungsdatei erstellen. Diese wird unter /usr/rsbac/TightGate/packages / abgelegt.		**E0**	
Starte RSBAC-Menü	Übergang in das RSBAC-Konfigurationsmenü. **Warnung:** Einstellungen nur durch den technischen Kundendienst der m-privacy GmbH. Unsachgemäße Änderungen am Sicherheitssystem von TightGate®-Pro Server bergen erhebliche Sicherheitsrisiken für das interne Netzwerk und die darin befindlichen Arbeitsplatzrechner. Weiterhin können schwerwiegende Störungen des Produktivbetriebs auftreten.		**E1** **E2**	
Konsole	Aufruf der Konsole für den Administrator ***security***.		**E0**	
RC Konfiguration	Anzeige der definierten RSBAC-Typen und -Rollen im System.		**E0**	
RC-Debug-Modus an	Einschalten des ausführlichen Debuggings für das RSBAC RC-Modul. **Achtung:** Einschalten dieser Menüoption erhöht die Anzahl der Meldungen im Syslog erheblich. Eine „überlaufende“ Logpartition kann das Systemverhalten negativ beeinflussen.		**E0**	
RC-Debug-Modus aus	Ausschalten des ausführlichen Debuggings für das RSBAC RC-Modul.		**E0**	
Globaler Softmode an	Abschalten des RSBAC-Sicherheitssystems - nur in Ausnahmefällen und außerhalb des Produktivbetriebs anzuwenden. **Warnung:** Zentrale Sicherheitseinrichtungen von TightGate®-Pro Server werden außer Kraft gesetzt. Das Schutzniveau des ReCoBS-Servers sowie des internen Netzwerks ist stark vermindert. Es besteht weiterhin die Gefahr von Betriebsstörungen und Datenverlust bei Aktivierung des globalen Softmodes im Produktivbetrieb!		**E2**	
Globaler Softmode aus	Abschalten des Softmodes. Das RSBAC-Sicherheitssystem ist wieder aktiv.		**E0**	
RC-Softmode an	Abschalten RC-Modul des RSBAC-Systems - nur in Ausnahmefällen und außerhalb des Produktivbetriebs anzuwenden. **Warnung:** Zentrale Sicherheitseinrichtungen von TightGate®-Pro Server werden außer Kraft gesetzt. Das Schutzniveau des ReCoBS-Servers sowie des internen Netzwerks ist stark vermindert. Es besteht weiterhin die Gefahr von Betriebsstörungen und Datenverlust bei Aktivierung des RC-Softmode im Produktivbetrieb!		**E2**	
RC-Softmode aus	Abschalten des RC-Softmode. Das RC-Modul ist wieder aktiv.		**E0**	
Revision-Passwort	Ändern des Passworts für den Administrator ***revision***.		**E2** **E4**	

security		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Security-Passwort	Ändern des Passworts für den Administrator ***security***.		**E2** **E4**	

13.2 Der Administrator 'root'

Die Rolle ***root*** entspricht im wesentlichen der des klassischen Verwalters für Systemdienste. Als Administrator ***root*** können installierte Systemdienste gestartet und angehalten werden, es können Tests mit Systemwerkzeugen durchgeführt und Systemdienste konfiguriert werden. Im Gegensatz zum gleich bezeichneten und in seinem Kompetenzen unbeschränkten Administrator-Account eines konventionellen Linux-Systems unterliegt die Rolle ***root*** jedoch besonderen Beschränkungen. So kann der Administrator ***root*** insbesondere nicht auf die Verzeichnisse der Benutzer zugreifen, keine Programme mit RSBAC-Rechten ausstatten und keine RSBAC-Rechte ändern, diese jedoch einsehen.

Um den Status der Sicherheitsmodelle und Prozesse anzuzeigen sowie einen Einblick in das laufende System-Log zu nehmen, ist eine Anmeldung als Administrator ***root*** an der Konsole erforderlich.

root		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Ende	Verlassen des Menüs und Beenden des Zugangs als Administrator ***root***		**E2**	
Modul-Status	Anzeige des Status‘ der Sicherheitsmodule. **Warnung:** Stati im Produktivbetrieb müssen sein: Mode: „secure“ Softmode / Ind-Soft: „unavailable“ Switching on / off: „unavailable“ Module (alle!): „on“ Andernfalls können erhebliche Sicherheitsdefizite die Folge sein. Zudem besteht die Gefahr erheblicher Betriebsstörungen.		**E0**	
Prozess-Status	Anzeige des Status‘ aller laufenden Prozesse.		**E0**	
Systemprotokolle	Fortlaufende Anzeige der Systemmeldungen.		**E0**	
Konsole	Aufruf einer Konsole für den Administrator ***root*** .		**E0**	
Wartungs-Konsole	Aufruf einer Wartungskonsole für den Administrator ***root***. Wurde durch den Administrator ***security*** dem Administrator ***root*** die Wartungsrolle zugeteilt, so kann Letzterer mit erweiterten Berechtigungen im System arbeiten. Diese Funktion ist speziell für Wartungsaufgaben vorgesehen und sollte mit Umsicht eingesetzt werden. Die erweiterten Berechtigungen aufgrund der Wartungsrolle sind dem Anhang zu entnehmen.		**E0**	
Neustart	Neustart des ReCoBS-Servers, entweder sofort oder gemäß Terminierung.		**E1** **E2**	
Neustart abbrechen	Löschen eines geplanten Termins zum Neustart des ReCoBS-Servers.		**E2**	
Herunterfahren	Herunterfahren des ReCoBS-Servers.		**E2**	
Root-Passwort	Ändern des Passworts für den root-Zugang.		**E2** **E4**	

14 Clustereinstellungen

Ein Verbundrechnersystem oder Cluster bezeichnet eine Anzahl von Einzelrechnern, die über ein besonders leistungsstarkes Netzwerk zu einem logischen Verbund gekoppelt sind. Ein Rechnerverbund wird in der Regel als ein zusammenhängendes Gerät betrachtet. Rechnerverbünde zeichnen sich gegenüber Einzelsystemen durch höhere Leistungsfähigkeit und Verfügbarkeit aus.

Warnung: Die Grundeinstellungen des Rechnerverbunds sind bei betriebsbereiten Appliances werkseitig vorkonfiguriert und sollten nur durch den Kundendienst der m-privacy GmbH geändert werden. Unsachgemäße Änderungen gefährden den Betrieb des gesamten Clusters.

Die Konfiguration der Clustereinstellungen erfordert eine Anmeldung als Administrator ***config*** an der Konsole. Das Untermenü Cluster-Einstellungen befindet sich im Menü ***Einstellungen***. Die meisten Optionen gelten für den gesamten Rechnerverbund unabhängig von der Zahl seiner Nodes.

Hinweis: Einige der im Folgenden dargestellten Einstelloptionen werden in Abhängigkeit bestimmter Konfigurationen angezeigt, d. h. sie sind unter Umständen ausgeblendet.

config > Einstellungen > Cluster-Einstellungen		**Hinweise**		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Zurück	Rückkehr zum Hauptmenü.		**E0**	
Aktiviere TightGate-Cluster	Aktivierung oder Deaktivierung des Verbundrechnermodus‘.		**E1**	
Anzahl Nodes*	Gibt die Anzahl der Einzelrechner (Nodes) im Verbund an.		**E6**	
Cluster-Basis-IP*	Erste IPv4-Adresse des Clusternetzwerkes. Die Standardadresse ist 192.168.111.1.		**E5**	**F5**
Cluster-Basis-Name*	Im Cluster verwendeter Rechnername ohne die angehängte laufende Nummer. Aus diesem Namen werden die verwendeten Rechnernamen im Cluster generiert.		**E4**	
Cluster-Partner-IP-Netzwerk*	Verbundinternes Netzwerk, über das die einzelnen TightGate®-Pro-Serversysteme (Nodes) des Verbunds kommunizieren. **Achtung:** Die IPv4-Adressen der Nodes im Clusternetzwerk müssen immer aufeinander folgende IPv4-Adressen erhalten. Diese sind unabhängig vom Klienten-Netzwerk.		**E5**	
Verteilte Gluster-Datenhaltung*	Gibt an, ob die Datenhaltung über alle TightGate®-Pro-Systeme (Nodes) verteilt werden soll (in der Regel erforderlich).		**E1**	
Gluster-Sync-Prüfziele	Interne Einstellung, keine Änderung erforderlich.			
Gluster-Sync erlaubt	Interne Einstellung, keine Änderung erforderlich.			
Verteilte CEPH-Datenhaltung*	Funktion derzeit nicht implementiert, Einstelloption für zukünftige Erweiterung. **Achtung:** Muss stets auf „nein“ stehen, um Funktionsstörungen von TightGate®-Pro Server zu vermeiden.			

config > Einstellungen > Cluster-Einstellungen		Hinweise		
Menüpunkt	**Beschreibung**	**C**	**E**	**F**
Aktiviere Cluster DNS Load Balancer	Aktivierung oder Deaktivierung des automatischen Lastverteilers auf diesem Cluster-Knoten. Der DNS-Load-Balancer verteilt die VNC-Anmeldungen lastabhängig auf die einzelnen TightGate®-Pro-Nodes. **Hinweis:** Cluster-Knoten (Nodes) mit ausgeschöpftem Plattenplatz werden automatisch von der Lastverteilung ausgenommen, sodass sich keine weiteren VNC-Benutzer darauf anmelden können. Die Belegung der Festplatten kann über die Nagios-Systemüberwachung kontrolliert werden.		**E1**	
Cluster DNS-Domäne*	Domäne, unter der Load-Balancer erreichbar ist.		**E4**	
Cluster-Clienten-Basis-IP*	Erste IPv4-Adresse, die für Klienten zur Verfügung steht.		**E5**	

14.1 Beispiel eines Rechnerverbunds

In dem Beispiel soll ein Rechnerverbund (Cluster) aus 4 TightGate®-Pro-Systemen erstellt werden. Der DNS-Name, über den der Verbund angesprochen werden soll, lautet internet.tightgate. Das VNC-Klientennetzwerk ist 10.0.1.0/24.

A-priori-Festlegungen:

- IPv4-Adresse der TightGate®-Pro-Systeme im LAN
- Welche TightGate®-Pro-Systeme sind zur Lastverteilung bestimmt?

Beispielhafte Übersicht für die Clustereinstellungen:

System-Nr.	System-Name	Cluster-IP	LAN-IP	Aktiviere DNS-Load-Balancer
1	tgpro1	192.168.111.1	10.0.1.201	ja
2	tgpro2	192.168.111.2	10.0.1.202	nein
3	tgpro3	192.168.111.3	10.0.1.203	ja
4	tgpro4	192.168.111.4	10.0.1.204	nein

Diese Einstellungen werden in der Clusterkonfiguration als Administrator ***config*** für den ersten Node wie folgt eingetragen:

Menüpunkt	Parameter
Aktiviere TightGate®-Cluster	ja
Anzahl Nodes	4
Cluster-Basis-IP	192.168.111.1
Cluster-Basis-Name	tgpro1
Cluster-Partner-IP-Netzwerk	192.168.111.0/24
Verteilte Gluster-Datenhaltung	ja
Gluster-Sync-Prüfziele	kein Eintrag
Gluster-Sync erlaubt	ja
Verteile CEPH-Datenhaltung	nein

Aktiviere Cluster DNS Load Balancer	ja
Cluster DNS-Domäne	internet.tightgate
Cluster-Klienten-Basis-IP	10.0.1.201

Die Systeme 2-4 werden analog konfiguriert.

Exkurs: DNS-Domäne und DNS-Zonen-Forwarding

Damit der TightGate®-Pro-Cluster mit einem Namen angesprochen werden kann und eine Lastverteilung innerhalb des eingebauten Lastverteilungssystems funktioniert, muss im Netzwerk sichergestellt sein, dass der DNS-Name internet.tightgate über die DNS-Server unter den IP-Adressen 10.0.1.201 und 10.0.1.203 aufgelöst wird. Dies wird erreicht durch ein sogenanntes DNS-Zonen-Forwarding beim DNS-Server im Netzwerk. Ist das DNS-Zonen-Forwarding richtig konfiguriert, können sich die VNC-Klienten unter Angabe des Namens internet.tightgate direkt mit TightGate®-Pro Server verbinden. TightGate®-Pro Server selbst entscheidet, welche Systeme im Cluster stärker belastet sind und verteilt eingehende Anfragen auf Systeme mit weniger Last. Im Wartungsbetrieb befindliche Knoten werden automatisch übergangen.

Hinweis: Die Anmeldung erfolgt je nach Lastzustand automatisch an unterschiedlichen Nodes.